(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－165081
（P2002－165081A）
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		５Ｂ０５７
Ｇ０６Ｔ　1/00	５００	Ｇ０６Ｔ　1/00	５００Ｂ	５Ｃ０６３
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｃ０７６
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		５Ｊ１０４
Ｈ０４Ｎ　7/08		Ｈ０４Ｎ　7/08	Ｚ	

審査請求　未請求　請求項の数30　ＯＬ　（全 26 頁）　最終頁に続く

(21)出願番号　特願2000－361433(P2000－361433)

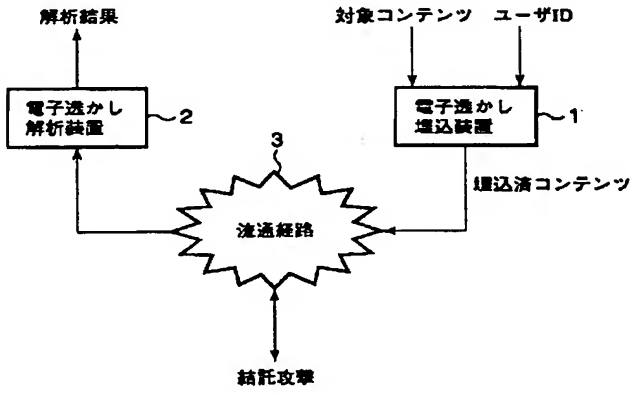
(22)出願日　平成12年11月28日(2000.11.28)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　村谷　博文
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B057 AA11 CA16 CA19 CB16 CE08 CH08 DA07 DA13
5C063 AB03 AC01 AC05 CA23 CA36 DA07 DA13 DB09
5C076 AA14 BA07
5J104 AA13 AA14

(54)【発明の名称】　電子透かしシステム、電子透かし解析装置、電子透かし解析方法及び記録媒体

(57)【要約】
【課題】　結託耐性符号の埋め込まれたデジタルコンテンツの複製物に対する結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステムを提供すること。
【解決手段】　電子透かし埋め込み装置１では、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に、該ユーザのユーザＩＤに一意に対応する結託耐性符号を埋め込む。コンテンツが流通経路３を経た後に、電子透かし解析装置２では、解析対象となったデジタルコンテンツの複製物から結託耐性符号を検出し、検出された符号を構成する複数の成分符号の各々について改ざん部分の位置に関係する位置情報を検出し、該位置情報に基づいて成分符号の改ざん部分の位置に関係する所定の統計量を求め、該所定の統計量に基づいて該デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する。



1

【特許請求の範囲】

【請求項１】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かしシステムであって、

デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する識別情報に対して、所定の方法に従って、複数の整数を割り当て、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、

生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、

生成された前記結託耐性符号を前記複製物に埋め込む第１のステップと、

解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、

検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出し、

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求め、

求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第２のステップとを有することを特徴とする電子透かしシステム。

【請求項２】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステムであって、

デジタルコンテンツの複製物に対応するユーザを特定する識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた複製物に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、

デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する前記識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、

生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、

生成された前記結託耐性符号を前記複製物に埋め込む第１のステップと、

解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、

検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求め、

2

求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、

この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、

求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第２のステップとを有することを特徴とする電子透かしシステム。

【請求項３】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置であって、

解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出する手段と、

検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出する手段と、

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求める手段と、

求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段とを備えたことを特徴とする電子透かし解析装置。

【請求項４】前記デジタルコンテンツの複製物は、該複製物がユーザへ渡されるのに先だって、

前記複製物に対応するユーザを特定する識別情報に対して、所定の方法に従って、複数の整数を割り当てる処理と、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成する処理と、

生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成する処理と、

生成された前記結託耐性符号を埋め込む処理とが行われたものであることを特徴とする請求項３に記載の電子透かし解析装置。

【請求項５】前記複製物に埋め込まれる前記結託耐性符号を構成する前記複数の成分符号の各々は、連続する所定のビット数の１または０のみからなるビット列を一単位として、該１または０のみからなるビット列を、該成分符号に対応する前記整数より１減じた個数だけ連接したものであって、かつ、０のみからなるか、１のみからなるか、または該成分符号のビット列中において該成分符号に対応する前記整数の値に応じた１ヶ所の位置でのみ０と１が隣接する符号であることを特徴とする請求項３または４に記載の電子透かし解析装置。

【請求項６】前記複製物から検出された前記符号を構成する前記複数の成分符号の各々について、該成分符号を構成する前記所定のビット数を一単位とするビット列に０と１が混在するものが検出された場合に、該ビット列が結託攻撃によって改ざんされた部分であると判断し、

3

改ざんされたビット列の範囲についての両端部分を特定可能な情報を、前記改ざん部分の位置に関係する位置情報として検出することを特徴とする請求項５に記載の電子透かし解析装置。

【請求項７】前記複製物から検出された前記符号を構成する前記複数の成分符号の各々について、改ざんされた部分でないと判断された成分符号については、該成分符号が０のみからなる場合には、該成分符号の全ビット列についての二つの端部のうちの予め定められた一方の端部を、該成分符号が１のみからなる場合には、該成分符号の全ビット列についての二つの端部のうちの予め定められた他方の端部を、該成分符号が連続する複数の０と連続する複数の１とを連接したものである場合には、該連続する複数の０と連続する複数の１との境界部分を、前記改ざん部分の位置に関係する位置情報として検出することを特徴とする請求項６に記載の電子透かし解析装置。

【請求項８】検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、

求められた複数の前記最上位ビット側位置をそれぞれ規準化した値に対する第１の平均と、求められた複数の前記最下位ビット側位置をそれぞれ規準化した値に対する第２の平均との一方または両方を求め、

求められた前記第１の平均と前記第２の平均の一方または両方を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めることを特徴とする請求項３ないし７のいずれか１項に記載の電子透かし解析装置。

【請求項９】前記所定の関数は、前記複製物に対応するユーザを特定する識別情報に対して所定の方法に従って割り当てられた前記複数の整数の各々についてその値が全識別情報についてランダムに分布すると仮定した場合において、結託攻撃に用いられる複製物の個数を変化させたときに、各々の個数と、その個数について確率的に期待される前記第１の平均の値およびまたは前記第２の平均の値との関係に基づくものであることを特徴とする請求項８に記載の電子透かし解析装置。

【請求項１０】検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、

求められた複数の前記最上位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット側にあるものの個数についての第１の比と、求められた複数の前記最下位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット側にあるものの個数についての第２の比との一方または両方を求め、

前記第１の比と前記第２の比の一方または両方を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めることを特徴とする請求項３ないし７のいずれか１項に記載の電子透かし解析装置。

【請求項１１】前記所定の関数は、前記複製物に対応するユーザを特定する識別情報に対して所定の方法に従って割り当てられた前記複数の整数の各々についてその値が全識別情報についてランダムに分布すると仮定した場合において、結託攻撃に用いられる複製物の個数を変化させたときに、各々の個数と、その個数について確率的に期待される前記第１の比の値およびまたは前記第２の比の値との関係に基づくものであることを特徴とする請求項８に記載の電子透かし解析装置。

【請求項１２】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置であって、

解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出する手段と、

検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求める手段と、

求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類する手段と、

この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求める手段と、

求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段とを備えたことを特徴とする電子透かし解析装置。

【請求項１３】前記デジタルコンテンツの複製物は、該複製物がユーザへ渡されるのに先だって、

前記複製物に対応するユーザを特定する識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた複製物に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当てる処理と、

デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する前記識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当てる処理と、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成する処理と、

生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成する処理と、

4

5

生成された前記結託耐性符号を埋め込む処理とが行われたものであることを特徴とする請求項１２に記載の電子透かし解析装置。

【請求項１４】前記弱識別子と前記非弱識別子との分類結果に基づいて、弱識別子に分類された識別子の数と、非弱識別子に分類された識別子の数との比を求め、

求められた前記比を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めることを特徴とする請求項３ないし７のいずれか１項に記載の電子透かし解析装置。

【請求項１５】前記所定の関数は、結託攻撃に用いられる複製物の個数を変化させたときに、各々の個数と、その個数について確率的に期待される前記比の値との関係に基づくものであることを特徴とする請求項１４に記載の電子透かし解析装置。

【請求項１６】前記結託攻撃に用いられた複製物の数の推定値を求める代わりに、前記結託攻撃に用いられた複製物の数の大小レベルを示す情報を求めることを特徴とする請求項１４に記載の電子透かし解析装置。

【請求項１７】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析方法であって、

解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出し、

検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出し、

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求め、

求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定することを特徴とする電子透かし解析方法。

【請求項１８】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析方法であって、

解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、

検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求め、

求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、

この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、

求められた前記弱識別子と非弱識別子とに関する所定の

6

統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定することを特徴とする電子透かし解析方法。

【請求項１９】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取り可能な記録媒体であって、

解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出するための機能と、

検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出するための機能と、

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求めるための機能と、

求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項２０】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取り可能な記録媒体であって、

解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出するための機能と、

検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求めるための機能と、

求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類するための機能と、

この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求めるための機能と、

求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項２１】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムであって、

解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出するための機能と、

検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出するための機能と、

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求めるための機能と、
求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラム。

【請求項２２】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムであって、
解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出するための機能と、
検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求めるための機能と、
求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類するための機能と、
この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求めるための機能と、
求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラム。

【請求項２３】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、
対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、
割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、
生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、
生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、
解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、
検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第２のステップとを有することを特徴とする化学物質透かしシステム。

【請求項２４】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、
対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子である

として誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、
前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、
割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、
生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、
生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、
解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、
検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第２のステップとを有することを特徴とする化学物質透かしシステム。

【請求項２５】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、
対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、
割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、
生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、
解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、
検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出し、
前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求め、
求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数を推定する第２のステップとを有することを特徴とする化学物質透かしシステム。

【請求項２６】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、
対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、

前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、
割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、
生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、
生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、
解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、
検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求め、
求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、
この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、
求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数を推定する第２のステップとを有することを特徴とする化学物質透かしシステム。

【請求項２７】前記結託耐性符号の前記化学物質製品への埋め込みは、該化学物質製品の持つ構造のうち透かしの埋め込みに使用される特定部位の構造を当該結託耐性符号の値に基づいて変換することによって行われることを特徴とする請求項２３ないし２６のいずれか１項に記載の化学物質透かしシステム。

【請求項２８】前記化学物質製品が複数の合成材料を合成してなるものである場合に、前記結託耐性符号の該化学物質製品への埋め込みは、個々の合成材料について予め該結託耐性符号の取りうる値の各々に対応させて特定部位の構造を変換させたものを用意しておき、該結託耐性符号の値に基づいて該当する個々の合成材料を選択し、選択した合成材料を合成することによって行われることを特徴とする請求項２３ないし２６のいずれか１項に記載の化学物質透かしシステム。

【請求項２９】前記結託耐性符号の前記化学物質製品からの検出は、該化学物質製品の持つ構造のうち透かしの埋め込みに使用される特定部位の構造を解析することによって行われることを特徴とする請求項２３ないし２６のいずれか１項に記載の化学物質透かしシステム。

【請求項３０】前記化学物質製品の持つアミノ酸の配列構造における特定部位のアミノ酸の置換後の種類によって前記結託耐性符号の内容を表現するようにしたことを特徴とする請求項２７ないし２９のいずれか１項に記載の化学物質透かしシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、結託耐性符号の埋め込まれたデジタルコンテンツの複製物に対する結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステム、電子透かし解析装置及び電子透かし解析方法に関する。

【０００２】

【従来の技術】デジタルコンテンツ（例えば、静止画、動画、音声、音楽等）は、多数のデジタルデータで構成された構造を持つ。そして、その構造の中には、データを変更しても、当該デジタルコンテンツの作品の同一性あるいは経済的価値を保持できる部分がある。そのような許容された範囲内のデータを変更するによって、デジタルコンテンツに、種々の情報を埋め込むことができる。このような技術は、電子透かしと呼ばれる。

【０００３】電子透かし技術によって、デジタルコンテンツに、様々な透かし情報（例えば、コンテンツの著作権者やユーザの識別情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）を、様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込み、検出・利用することができる。

【０００４】ここでは、例えば同一のデジタルコンテンツを多数のユーザを対象として配給するときに適用される技術として、デジタルコンテンツの複製物に、当該複製物を個々に識別するための情報（例えば、ユーザＩＤに一意に対応する透かし情報）を埋め込む場合を考える。

【０００５】デジタルコンテンツの複製物に固有の識別情報を埋め込む手法は、そのデジタルコンテンツの複製物が更に複製されて海賊版として出回ったときに、該海賊版から識別情報を検出することによって流出元ユーザを特定することができることから、デジタルコンテンツの違法コピーに対する事前の抑制として機能するとともに、著作権侵害が発生したときの事後の救済にも役立つことになる。

【０００６】また、あるユーザがデジタルコンテンツの複製物に埋め込まれた識別情報を無効するためには、ユーザにはどの部分が識別情報を構成するビットであるか分からないので、当該デジタルコンテンツの複製物に相当の改変を加える必要があり、そうすると、当該デジタルコンテンツの経済的価値を損なってしまうので、違法コピーの動機付けを奪うことができる。

【０００７】このような状況において違法コピーを可能ならしめる方法として出現したのが、「結託攻撃（ｃｏｌｌｕｓｉｏｎ　ａｔｔａｃｋ）」である。

【０００８】結託攻撃は、異なる複製物には異なる識別情報が埋めこまれていることを利用するものであり、例えば、複数人で複製物を持ちよって、それらをビット単

11

位で比較することによって、デジタルデータの値が異なる部分を見つけ出し、その部分を改ざん（例えば、多数決、少数決、ランダマイズ等）することによって、識別情報を改ざん、消失させるという方法である（なお、具体的な比較操作は行わず、コンテンツ間で画素値を平均化するなどの操作を行って、同様の結果を得る場合もある）。

【０００９】例えば簡単な例で示すと、Ａ氏、Ｂ氏、Ｃ氏の複製物にそれぞれ、

００…００…

００…１１…

１１…００…

という識別情報が埋め込まれていた場合に、例えば、

１０…０１…

という、Ａ氏、Ｂ氏、Ｃ氏のいずれとも異なる識別情報が埋め込まれたコンテンツを出現させることができてしまう。

【００１０】そこで、結託攻撃に対する耐性、すなわち結託攻撃を受けても結託者の全部または一部を特定できるような性質を持つ符号（以下、結託耐性符号と呼ぶ）を電子透かしとして埋め込む方法および該結託耐性符号に基づく追跡アルゴリズム（ｔｒａｃｉｎｇ　ａｌｇｏｒｉｔｈｍ；結託攻撃に用いられたコンテンツに埋め込まれた識別番号を特定し、結託者のユーザＩＤを特定するためのアルゴリズム）が種々提案されている。例えば、その一つにｃ－ｓｅｃｕｒｅ符号がある(D.Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data," CRYPTO' 95, 180-189, 1995.)。

【００１１】

【発明が解決しようとする課題】結託攻撃に対する耐性をより強くする、すなわち結託者を特定できなくなる結託数の上限数をより増やすためには、コンテンツに埋め込む符号長をより長くする必要があり、一方、コンテンツに埋め込む符号長にも制限があるので、この種の結託耐性符号およびその結託耐性符号に基づく追跡アルゴリズムでは、符号長を削減するために、結託攻撃に利用された複製物の数に上限を設けている（なお、ｃ－ｓｅｃｕｒｅのｃは、高々ｃ個までの複製物を用いた結託攻撃に対して有効であるという意味である）。もし結託攻撃が許容されている個数を越える数の複製物を用いて行われた場合には、追跡アルゴリズムは、結託攻撃に関与した複製物の識別番号として、誤って、結託攻撃に関与したのではない複製物の識別番号を出力し、結託者でないものが結託者として特定されてしまう、という誤判定が発生することがあり得る。なお、結託攻撃においてそれに関与した複製物以外の複製物の識別番号と同一の識別番号を持つ複製物が生成される可能性と、許容個数以下での誤判定の可能性は、結託耐性符号の設計によって確率的にかなり低く抑えられるので、誤判定は、主に許容個数を越える結託攻撃によって発生する。

12

【００１２】しかし、現実に許容個数までの複製物で結託攻撃が行われたか否かは、攻撃者（結託者）のみが知る情報である。攻撃者は、複製物の偽造によって不法に利益を得ることを目的としているため、結託攻撃に用いた複製物の個数を自ら公開することはおよそ考えられない。

【００１３】したがって、該結託耐性符号の復号を行う追跡アルゴリズムが結託に関与した複製物の識別番号（あるいは、該識別番号に対応する結託者のユーザＩＤ）を出力したとしても、それが、正しく複製物あるいは結託者を特定しているのか、それとも、結託攻撃が許容されている個数を越える数の複製物を用いて行われたために、誤って、結託に使われていなかった複製物あるいはそのユーザを特定してしまったのかを、判別することができない、という問題点がある。

【００１４】また、この問題を回避するためには、現実的に結託者が準備することができそうな複製物の個数を想像し、その個数以上の許容個数となるように結託耐性符号を設計するより他なく、どうしても、大きな許容個数を設定することになってしまい、その結果、符号長も大きくなってしまう。

【００１５】本発明は、上記事情を考慮してなされたもので、結託耐性符号の埋め込まれたデジタルコンテンツの複製物に対する結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステム、電子透かし解析装置及び電子透かし解析方法を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明は、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かしシステムであって、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記複製物に埋め込む第１のステップと、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出し、前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求め、求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第２のステップとを有することを特徴とする。

【００１７】また、本発明は、結託攻撃に用いられたデ

ジタルコンテンツの複製物の数を推定可能な電子透かしシステムであって、デジタルコンテンツの複製物に対応するユーザを特定する識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた複製物に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する前記識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記複製物に埋め込む第１のステップと、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求め、求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第２のステップとを有することを特徴とする。

【００１８】また、本発明は、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置／装置であって、解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出する手段／ステップと、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出する手段／ステップと、前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求める手段／ステップと、求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段／ステップとを備えたことを特徴とする。

【００１９】好ましくは、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、求められた複数の前記最上位ビット側位置をそれぞれ規準化した値に対する第１の平均と、求められた複数の前記最下位ビット側位置をそれぞれ規準化した値に対する第２の平均との一方または両方を求め、求められた前記第１の平均と前記第２の平均の一方または両方を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めるようにしてもよい。

【００２０】また、本発明は、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、求められた複数の前記最上位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット側にあるものの個数についての第１の比と、求められた複数の前記最下位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット側にあるものの個数についての第２の比との一方または両方を求め、前記第１の比と前記第２の比の一方または両方を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めるようにしてもよい。

【００２１】また、本発明は、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置／方法であって、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出する手段／ステップと、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求める手段／ステップと、求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類する手段／ステップと、この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求める手段／ステップと、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段／ステップとを備えたことを特徴とする。

【００２２】好ましくは、前記弱識別子と前記非弱識別子との分類結果に基づいて、弱識別子に分類された識別子の数と、非弱識別子に分類された識別子の数との比を求め、求められた前記比を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めるようにしてもよい。

【００２３】好ましくは、前記結託攻撃に用いられた複製物の数の推定値を求める代わりに、前記結託攻撃に用いられた複製物の数の大小レベルを示す情報を求めるようにしてもよい。

【００２４】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り

当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第２のステップとを有することを特徴とする。

【００２５】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第２のステップとを有することを特徴とする。

【００２６】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関係する位置情報を検出し、前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関係する所定の統計量を求め、求められた前記改ざん部分の位置に関係する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数を推定する第２のステップとを有することを特徴とする。

【００２７】化学物質透かしシステム。

【００２８】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を連接して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第１のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求め、求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数を推定する第２のステップとを有することを特徴とする。

【００２９】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００３０】本発明によれば、結託耐性符号の埋め込まれたデジタルコンテンツの複製物から検出した符号についての統計的な手法に基づく推定（例えば、結託耐性符号における改ざん部分の分布の偏り、あるいは検出された識別子における弱識別子の比率などに関する統計的性質等に基づく推定）を行うことによって、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定することができる。これによって、追跡アルゴリズムの追跡結果の正誤に関する評価や、結託数自体の情報収集などができるようになる。

【００３１】

【発明の実施の形態】以下、図面を参照しながら発明の

実施の形態を説明する。

【００３２】本発明は、同一のデジタルコンテンツの複製物（例えば、静止画、動画、音声、音楽等）の各々に対して、少なくとも、複製物ごとに異なるユーザ識別符号（後述するように、当該複製物に対応するユーザすなわち当該複製物を利用することになるユーザ（例えば、当該複製物を譲渡するユーザ、あるいは当該複製物を貸し渡すユーザ）のユーザ識別子（ユーザＩＤ）に一意に対応する識別情報であって結託耐性符号に基づくもの）を透かし情報として埋め込み、検出する場合に適用可能である。

【００３３】もちろん、同一のデジタルコンテンツの複製物の各々に対して、さらに、その他の様々な透かし情報（例えば、コンテンツの著作権者の識別情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）を様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込み、検出するものであってもよいが、以下では、ユーザ識別符号に関係する部分を中心に説明する（その他の透かし情報を利用する場合における当該その他の透かし情報に関係する部分の構成は特に限定されない）。

【００３４】以下で示す構成図は、装置の機能ブロック図としても成立し、また、ソフトウェア（プログラム）の機能モジュール図あるいは手順図としても成立するものである。

【００３５】図１に、本発明の実施の形態に係る電子透かし埋込装置と電子透かし解析装置が適用されるシステムの概念図を示す。

【００３６】電子透かし埋込装置１と電子透かし解析装置２は、コンテンツ提供側に備えられ、管理される。電子透かし埋込装置１においてデジタルコンテンツに所望の透かしデータを埋め込む方法や、電子透かし解析装置２においてデジタルコンテンツから該透かしデータ自体を取り出す方法は、基本的には任意である（例えば、“松井甲子雄著、「電子透かしの基礎」、森北出版、１９９８年”等参照）。電子透かし埋込装置１は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。同様に、電子透かし解析装置２は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。また、電子透かし埋込装置１および電子透かし解析装置２をコンテンツ提供側で用いる場合には、それらを一体化して実現することも可能である。

【００３７】図２に、電子透かし埋込装置１の構成例を示す。この電子透かし埋込装置１は、ユーザ識別符号として埋め込むべき透かし情報である、ユーザＩＤに対応する結託耐性符号を生成する符号生成部１１と、生成された結託耐性符号（埋め込み符号）を対象コンテンツに埋め込む符号埋込部１２とから構成される。

【００３８】電子透かし埋込装置１は、対象コンテンツと、これに埋め込むべき対象ユーザのユーザＩＤとが与えられると、該ユーザＩＤに対応する結託耐性符号を生成し、ユーザ識別符号として該結託耐性符号が埋め込まれたコンテンツを、該ユーザＩＤのユーザ向けの複製物として出力する。他の透かし情報を利用する場合には、その際に、必要に応じて他の透かし情報が埋め込まれる。

【００３９】電子透かし埋込装置１により得られた各ユーザ向けのコンテンツの複製物は、記憶媒体や通信媒体などを媒介とした流通経路３を経てそれぞれ流通する。複数の複製物を用いた結託攻撃は、この流通経路３にて行われる。

【００４０】図３、図４に、電子透かし解析装置２の構成例を示す。

【００４１】図３、図４に示されるように、電子透かし解析装置２は、検出対象となるコンテンツからユーザ識別符号（埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの）を抽出する符号抽出部２１と、検出対象となるコンテンツについて、結託攻撃に使用された複製物の個数を推定する結託数推定部２２と、所定の追跡アルゴリズムを実行して、結託攻撃に用いられたであろう複製物の結託耐性符号を特定し、該結託耐性符号に対応するユーザＩＤ（ユーザＩＤが復元できない場合のある追跡アルゴリズムでは、結託攻撃に用いられたであろう結託耐性符号に対応するユーザＩＤ、またはユーザＩＤを復元できなかった旨）を特定する（なお、結託攻撃に用いられたであろう結託耐性符号自体を求めずに、直接、対応するユーザＩＤを求めるようにしてもよい）追跡アルゴリズム処理部２３とを備える。なお、本実施形態では、結託攻撃がなされなかった場合、を、結託攻撃に使用された複製物の個数＝１として扱うものとする。

【００４２】ここで、電子透かし解析装置２の結託数推定部２２には、（１）結託数推定部２２単独で（追跡アルゴリズム処理部２３の結果を利用することなしに）、検出対象となるコンテンツから、ユーザ識別符号（埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの）を取り出し、取り出したユーザ識別符号を解析することによって、結託攻撃に使用された複製物の個数を推定する形態（結託数推定部の第１の態様）と、（２）追跡アルゴリズム処理部２３から出力された追跡結果（例えば結託者の全部または一部のユーザＩＤ）に基づいて、結託攻撃に使用された複製物の個数を推定する形態（結託数推定部の第２の態様）とがある。図３は、結託数推定部の第１の態様の場合の構成例であり、図４は、結託数推定部の第１の態様の場合の構成例である。

【００４３】結託耐性符号や追跡アルゴリズムは、基本的には、どのようなものでも適用可能であり、特に限定

されない。

【００４４】なお、図３や図４において、さらに、結託数推定部２２の結果および追跡アルゴリズム処理部２３の結果を総合的に判断した判定結果を出力する総合判定部を備えても良い。加工処理部は、例えば、推定結託数が許容数以下で且つ結託者のユーザＩＤ（の集合）が得られた場合には、当該結託者のユーザＩＤ（の集合）を出力し（または、これに加えて推定結託数を出力し）、推定結託数が許容数を越え且つ結託者のユーザＩＤ（の集合）が得られた場合には、推定結託数オーバーによる判定不能である旨（または、これに加えて推定結託数）を出力する。もちろん、その他の総合判定結果の生成の仕方も可能である。

【００４５】なお、上記の（１）の場合には、結託数推定部２２による処理と、追跡アルゴリズム処理部２３による処理は、いずれを先に行ってもよいし、並列的に行ってもよい。

【００４６】また、上記の（１）の場合には、結託数推定部２２を持ち且つ追跡アルゴリズム処理部２３を持たない電子透かし解析装置２もあり得る。図５に、この場合の構成例を示す。

【００４７】本実施形態によれば、電子透かし解析装置２は結託数推定部２２によって結託攻撃に用いられたであろう複製物の個数を推定することができ、これによって追跡アルゴリズムの追跡結果の正誤に関する評価や、結託数自体の情報収集などができるようになる。

【００４８】以下では、電子透かし埋込装置１についてより詳細に説明する。

【００４９】図６に、概略的な手順の一例を示す。

【００５０】符号生成部１１は、まず、対象複製物に、埋め込むべきユーザＩＤに対応する、Ｍ（Ｍは複数）個の整数Ａ（１）、Ａ（２）、…、Ａ（Ｍ）を求める（ステップＳ１）。該Ｍ個の整数は、予め求めて記憶しておく方法と、必要時に求める方法とがある。

【００５１】各ｉ（ｉ＝１～Ｍ）におけるそれぞれの整数Ａ（ｉ）は、０～Ｎ（ｉ）－１のいずれかの値を取るものとする。ここで、Ｎ（１）、Ｎ（２）、…、Ｎ（Ｍ）は、予め定められた相互に異なる正整数とする。より好ましくは、Ｎ（１）、Ｎ（２）、…、Ｎ（Ｍ）は、互いに素である。

【００５２】ユーザＩＤに対応するＭ個の整数Ａ（ｉ）の各々には、０～Ｎ（ｉ）－１の範囲でランダムに値を割り当てる方法と、０～Ｎ（ｉ）－１の範囲で一定の規則に従って値を割り当てる方法とがある。また、いずれも場合についても、各ユーザＩＤには、互いにＡ（１）、Ａ（２）、…、Ａ（Ｍ－１）のうちの少なくと＊

＊も一つが相違するように排他的に割り当てる方法と、Ａ（１）、Ａ（２）、…、Ａ（Ｍ）のすべてを同一とするＭ個の整数の組を複数のユーザＩＤに重複に割当てることを許す方法とがある。

【００５３】排他的に値を割り当てる方法には、例えば、ユーザＩＤの値として、０～Ｎ（１）×Ｎ（２）×・・・×Ｎ（Ｍ）－１の範囲の整数の全部または一部を使用するものとし、Ｍ個の整数Ａ（ｉ）の各々について、対象ユーザＩＤをＮ（ｉ）で割ったときの余りを、該ユーザＩＤに対応するＡ（ｉ）の値とする方法がある。

【００５４】なお、ユーザＩＤから、該ユーザＩＤに対応する整数Ａ（１）、Ａ（２）、…、Ａ（Ｍ）の組を算出できない方法を用いる場合には、各ユーザＩＤと、該ユーザＩＤに対応する整数Ａ（１）、Ａ（２）、…、Ａ（Ｍ）の組との対応関係情報を保存しておく必要がある。また、ユーザＩＤから、該ユーザＩＤに対応する整数Ａ（１）、Ａ（２）、…、Ａ（Ｍ）の組を算出できる方法を用いる場合には、各ユーザＩＤと、該対応関係情報を保存せずに必要に応じて再計算するようにしてもよいし、該対応関係情報を保存しておいてこれを参照するようにしてもよい。

【００５５】次に、符号生成部１１は、対象複製物に埋め込むべきユーザＩＤに対応する、Ｍ個の整数Ａ（１）、Ａ（２）、…、Ａ（Ｍ）から、該ユーザＩＤに対応する結託耐性符号を生成する（ステップＳ２）。各ユーザＩＤに対応する結託耐性符号は、予め生成して記憶しておく方法と、必要時に生成する方法とがある。

【００５６】各ユーザＩＤに対応する結託耐性符号は、該ユーザＩＤに対応するＭ個の整数Ａ（１）、Ａ（２）、…、Ａ（Ｍ）の各々について、対応する成分符号Ｗ（１）、Ｗ（２）、…、Ｗ（Ｍ）を求め、それらを連結することによって生成する。

【００５７】整数Ａ（ｉ）に対応する成分符号Ｗ（ｉ）としては、例えば、Γ0(ｎ，ｄ)符号（１または０のみからなる連続したｄビットを一つの単位Ｂ（ｊ）とし、Ｂ（０）～Ｂ（ｎ－２）を連結したもの；ただし、Ｂ（０）～Ｂ（ｎ－２）は、すべてが０のみからなるか、すべてが１のみからなるか、またはＢ（０）～Ｂ（ｍ）までは０のみからなり且つＢ（ｍ）～Ｂ（ｎ－２）までは１のみからなるものである）を用いることができる。例えば、対象ユーザＩＤをＮ（ｉ）で割った余りを該ユーザＩＤに対応する整数Ａ（ｉ）の値とする方法の場合の簡単な例を示すと、Ｎ（１）＝５の場合、ｎ＝５となり、ｄ＝３とすると、Γ0(５，３)符号は、以下のようになる。

Ａ（１）＝０のとき　：　Ｗ（１）＝１１１　１１１　１１１　１１１
Ａ（１）＝１のとき　：　Ｗ（１）＝０００　１１１　１１１　１１１
Ａ（１）＝２のとき　：　Ｗ（１）＝０００　０００　１１１　１１１
Ａ（１）＝３のとき　：　Ｗ（１）＝０００　０００　０００　１１１

Ａ（１）＝４のとき　：　Ｗ（１）＝０００　０００　０００　０００

このようにして求めた各Ａ（ｉ）に対応する成分符号Ｗ（ｉ）を連結することによって、結託耐性符号を生成することができる。

【００５８】この符号では１と０はそれぞれｄビットを単位として連続するように配置され、ｄビット未満の数の１や０が孤立して存在することはない（上記の例では、３ビット未満の数の１や０が孤立して存在することはないことがわかる）。したがって、ｄビット未満の数の１や０が孤立して存在する場合には、結託攻撃がなされたことが推定される（ｄビット未満の数の１や０が孤立して存在しない場合には、結託攻撃がなされなかったことが推定される）。

【００５９】このようにして生成された結託耐性符号は、電子透かし埋込装置１の符号埋め込み部１２によって、対象コンテンツに埋め込まれる（ステップＳ３）。

【００６０】図７に、符号生成部１１の一構成例を示す。

【００６１】この符号生成部１１は、それぞれｋ′（＝Ｍ）個の法記憶部１２１－１，１２１－２，…，１２１－ｋ′、剰余計算部１２２－１，１２２－２，…，１２２－ｋ′、成分符号生成部１２４－１，１２４－２，…，１２４－ｋ′と、符号パラメータ記憶部１２３及び符号連接部１２５からなる。

【００６２】法記憶部１２１－１，１２１－２，…，１２１－ｋ′には、互いに素の関係にある整数、この例では相異なるｋ′個の素数ｐｉ（＝Ｎ（ｉ））（ｉ＝１，２，…，ｋ′）が記憶されており、これらの素数ｐｉが剰余計算部１２２－１，１２２－２，…，１２２－ｋ′に法として供給される。剰余計算部１２２－１，１２２－２，…，１２２－ｋ′は、入力されるユーザＩＤ＝ｕに対して、素数ｐｉを法とする剰余ｕｉ＝ｕ　ｍｏｄ　ｐｉ（ｉ＝１，２，…，ｋ′）をそれぞれ求める。すなわち、入力されたユーザＩＤに対応した複数の整数要素の組として、剰余計算部１２２－１，１２２－２，…，１２２－ｋ′により剰余ｕｉ＝ｕ　ｍｏｄ　ｐｉ（ｉ＝１，２，…，ｋ′）が計算される。なお、この例では、ｐｉ（ｉ＝１，２，…，ｋ′）は、素数としたが、互いに素な整数であってもよい。

【００６３】成分符号生成部１２４－１，１２４－２，…，１２４－ｋ′は、ｋ′個の素数ｐｉ（ｉ＝１，２，…，ｋ′）に対して、符号パラメータ記憶部２３に記憶された符号パラメータｔに従って剰余計算部１２２－＊１，１２２－２，…，１２２－ｋ′により求められた剰余ｕｉ（ｉ＝１，２，…，ｋ′）を表す前述したΓ０（ｎ，ｄ）符号からなる成分符号Γ０（ｐｉ，ｔ）をそれぞれ生成する。すなわち、成分符号生成部１２４－１，１２４－２，…，１２４－ｋ′では、所定個数（ｎ）のユーザＩＤに対して剰余計算部１２２－１，１２２－２，…，１２２－ｋ′で計算される全ての剰余ｕｉ（ｉ＝１，２，…，ｋ′）の組を表現可能なｋ′個の成分符号のうちのｋ個の組み合わせがユーザＩＤを一意に表現できる成分符号Γ０（ｐｉ，ｔ）を各剰余に対応して生成する。

Ａ（１）＝７　ｍｏｄ　Ｎ（１）＝０
Ａ（２）＝７　ｍｏｄ　Ｎ（２）＝０
Ａ（３）＝７　ｍｏｄ　Ｎ（３）＝０

となる。

【００７１】図１０に、この例においてユーザＩＤ＝０～１４の各々について求められたＡ（１）、Ａ（２）、Ａ（３）を示す。

【００６４】符号連接部１２５は、成分符号生成部１２４－１，１２４－２，…，１２４－ｋ′により生成された各成分符号Γ０（ｐｉ，ｔ）を連接することによって、透かし情報である結託耐性符号を生成する。

【００６５】図８に、成分符号生成部１２４－１，１２４－２，…，１２４－ｋ′の一つ（１２４－ｉ）の構成を示す。符号パラメータをｔ、剰余をｕｉ、法をｐｉとすると、減算部１３１ではｐｉ－ｕｉ－１が求められる。“０”列生成部１３２では、符号パラメータｔと剰余ｕｉに基づきｔ×ｕｉビットの連続した“０”列が生成され、“１”列生成部１３３では、符号パラメータｔと減算部１３１からの出力ｐｉ－ｕｉ－１に基づきｔ×（ｐｉ－ｕｉ－１）ビットの連続した“１”列が生成される。そして、これらの“０”列と“１”列が連接部３４で連接され、ｔ×（ｐｉ－１）ビットのビット列がΓ０（ｎ，ｄ）符号からなる成分符号Γ０（ｐｉ，ｔ）として生成される。

【００６６】図９は、こうして生成される結託耐性符号の成分符号（結託攻撃を受ける前の成分符号）の一例を示している。０からｎ－１までのｎ個のユーザＩＤに対応して、Ｂ（０），…，Ｂ（ｎ－２）のブロック“０”列からなる成分符号が割り当てられている。

【００６７】ここで、上記の符号生成方法について数値を小さくとって簡単にした例を用いて説明する。

【００６８】まず、整数の個数Ｍを３とし、Ｎ（１）＝３、Ｎ（２）＝５、Ｎ（３）＝７とする。この場合、Ａ（１）は０～２のいずれか、Ａ（２）は０～４のいずれか、Ａ（３）は０～６のいずれかとなる。

【００６９】次に、Ｎ（１）×Ｎ（２）×Ｎ（３）－１＝１０４であるので、０～１０４の範囲の全部または一部をユーザＩＤとして用いる。ここでは、そのうち０～１４をユーザＩＤとして用いるものとする。

【００７０】例えば、ユーザＩＤ＝７の場合、

ｍｏｄ　３＝１、
ｍｏｄ　５＝２、
ｍｏｄ　７＝０、

【００７２】次に、Γ０（ｎ，ｄ）符号においてｄ＝３とした場合におけるＡ（１）＝０、Ａ（１）＝１、Ａ（１）＝２のそれぞれに対応する成分符号Ｗ１は、次のようになる（なお、分かりやすくするために、０または

１を、３ビット単位に分けて記述している）。

Ａ（１）＝０　：　Ｗ１＝１１１　１１１

Ａ（１）＝１　：　Ｗ１＝０００　１１１

Ａ（１）＝２　：　Ｗ１＝０００　０００

Ａ（２）＝０：　Ｗ２＝１１１　１１１　１１１　１１１

Ａ（２）＝１：　Ｗ２＝０００　１１１　１１１　１１１

Ａ（２）＝２：　Ｗ２＝０００　０００　１１１　１１１

Ａ（２）＝３：　Ｗ２＝０００　０００　０００　１１１

Ａ（２）＝４：　Ｗ２＝０００　０００　０００　０００

また、同様に、Ａ（３）＝０、Ａ（３）＝１、Ａ（３）＝２、Ａ（３）＝３、Ａ（３）＝４、Ａ（３）＝５、Ａ※

Ａ（３）＝０：　Ｗ３＝１１１　１１１　１１１　１１１　１１１　１１１

Ａ（３）＝１：　Ｗ３＝０００　１１１　１１１　１１１　１１１　１１１

Ａ（３）＝２：　Ｗ３＝０００　０００　１１１　１１１　１１１　１１１

Ａ（３）＝３：　Ｗ３＝０００　０００　０００　１１１　１１１　１１１

Ａ（３）＝４：　Ｗ３＝０００　０００　０００　０００　１１１　１１１

Ａ（３）＝５：　Ｗ３＝０００　０００　０００　０００　０００　１１１

Ａ（３）＝６：　Ｗ３＝０００　０００　０００　０００　０００　０００

したがって、例えば、ユーザＩＤ＝７の場合、Ａ（１）★

Ｗ１＝０００　１１１

Ｗ２＝０００　０００　１１１　１１１

Ｗ３＝１１１　１１１　１１１　１１１　１１１　１１１

となり、ユーザＩＤ＝７に対応する結託耐性符号は、それらを連結して、

000111　000000111111　1111111111111111

となる（なお、分かりやすくするために、Ｗ１～Ｗ３に対応する部分の境界で分けて記述している）。

【００７３】図１１に、この例において各ユーザＩＤ＝０～１４について求められた結託耐性符号を示す。

【００７４】次に、電子透かし解析装置２についてより詳細に説明する。

【００７５】ここで、上記の例を利用して、結託攻撃について説明する。

【００７６】例えば、上記のユーザＩＤ＝２のユーザが入手したコンテンツには、ユーザ識別符号として、

000000　000000111111　0000001111111111111

が埋め込まれている（図１０、図１１参照）。また、例えば、上記のユーザＩＤ＝３のユーザが入手したコンテンツには、ユーザ識別符号として、

111111　000000000111　000000000111111111

が埋め込まれている（図１０、図１１参照）。

【００７７】この場合に、ユーザＩＤ＝２のユーザとユーザＩＤ＝３の２人のユーザが持ちよったコンテンツを比較すると、上記３６ビットのうち、左から１～６番目、１３～１５番目、２５～２７番目が相違していることがわかる。そこで、それらが識別情報の一部と分かるため、１～６番目、１３～１５番目、２５～２７番目のうちの一部に改ざんが施され、例えば、次のような改変が施される。

010101　000000010111　0000001011111111111

＊また、同様に、Ａ（２）＝０、Ａ（２）＝１、Ａ（２）＝２、Ａ（２）＝３、Ａ（２）＝４のそれぞれに対応する成分符号Ｗ２は、次のようになる。

＊

Ａ（２）＝０：　Ｗ２＝１１１　１１１　１１１　１１１

Ａ（２）＝１：　Ｗ２＝０００　１１１　１１１　１１１

Ａ（２）＝２：　Ｗ２＝０００　０００　１１１　１１１

Ａ（２）＝３：　Ｗ２＝０００　０００　０００　１１１

Ａ（２）＝４：　Ｗ２＝０００　０００　０００　０００

※（３）＝６のそれぞれに対応する成分符号Ｗ２は、次のようになる。

Ａ（３）＝０：　Ｗ３＝１１１　１１１　１１１　１１１　１１１　１１１

Ａ（３）＝１：　Ｗ３＝０００　１１１　１１１　１１１　１１１　１１１

Ａ（３）＝２：　Ｗ３＝０００　０００　１１１　１１１　１１１　１１１

Ａ（３）＝３：　Ｗ３＝０００　０００　０００　１１１　１１１　１１１

Ａ（３）＝４：　Ｗ３＝０００　０００　０００　０００　１１１　１１１

Ａ（３）＝５：　Ｗ３＝０００　０００　０００　０００　０００　１１１

Ａ（３）＝６：　Ｗ３＝０００　０００　０００　０００　０００　０００

★＝１、Ａ（２）＝２、Ａ（３）＝０であるから、

１１１　１１１

同様に、ユーザＩＤ＝７のユーザとユーザＩＤ＝８との２人のユーザで、例えば、次のような改ざんが施される。

000010　000000101111　0101111111111111111

また、同様に、ユーザＩＤ＝３、４、５、６の４人のユーザによって、例えば、次のような改ざんが施される。

010101　010101010101　000000000010101010

次に、追跡アルゴリズムの概要を説明する。

【００７８】符号抽出部２１によって、検出対象となるコンテンツからユーザ識別符号（埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの）が抽出されると、追跡アルゴリズム処理部２３は、抽出された符号を解析することによって、結託攻撃に用いられたであろう複製物の結託耐性符号を推定し、該結託耐性符号に対応するユーザＩＤを推定する。

【００７９】ここで、図１２（ａ）に示すように、符号（生成された結託耐性符号、結託攻撃を受けた結託耐性符号）の成分符号（上記の例では３つの成分符号）の各々ごとについて、当該成分符号の両端の位置と、隣接する要素Ｂ（ｄ－１）とＢ（ｄ）との境界の位置を、数値化して表すものとする。すなわち、第ｉ番目の成分符号Ｗ（ｉ）の要素Ｂ（ｊ）の数をＮ（ｉ）－１個とし、図１２（ａ）でＮ（ｉ）をＮで表すものとすると、要素Ｂ（０）の左端の位置が０、要素Ｂ（ｄ－１）とＢ（ｄ）との境界の位置がｄ、要素Ｂ（Ｎ－２）の右端の位置がＮ－１で表される。

【００８０】そして、コンテンツから検出された符号の第ｉ番目の成分符号Ｗ（ｉ）を、左端のビットからみて

25

いったときにはじめて出現する、０のみからなる要素Ｂ（ｓ－１）と１を含む要素Ｂ（ｓ）との境界を求め、該境界に対応する上記の位置を示す値ｓを、Ａｍｉｎ（ｉ）で表すものとする。一方、右端のビットからみていったときにはじめて出現する、１のみからなる要素Ｂ（ｔ）と０を含む要素Ｂ（ｔ－１）との境界を求め、該境界に対応する上記の位置を示す値ｔを、Ａｍａｘ（ｉ）で表すものとする。

【００８１】例えば、図１２（ｂ）の符号の例では、Ａｍｉｎ（ｉ）＝２、Ａｍａｘ（ｉ）＝４となる。また、例えば、図１２（ｃ）の符号の例では、Ａｍｉｎ（ｉ）＝２、Ａｍａｘ（ｉ）＝２となる。また、例えば、図１２（ｄ）の符号の例では、Ａｍｉｎ（ｉ）＝４、Ａｍａｘ（ｉ）＝４となる。なお、第ｉ番目の成分符号Ｗ（ｉ）が０のみからなる場合には、Ａｍｉｎ（ｉ）＝Ａｍａｘ（ｉ）＝Ｎ（ｉ）－１となる。また、１のみからなる場合には、Ａｍｉｎ（ｉ）＝Ａｍａｘ（ｉ）＝０と＊

Ａ（３）＝０：	Ｗ３＝１１１	１１１	１１１	１１１	１１１	１１１
Ａ（３）＝１：	Ｗ３＝０００	１１１	１１１	１１１	１１１	１１１
Ａ（３）＝２：	Ｗ３＝０００	０００	１１１	１１１	１１１	１１１
Ａ（３）＝３：	Ｗ３＝０００	０００	０００	１１１	１１１	１１１
Ａ（３）＝４：	Ｗ３＝０００	０００	０００	０００	１１１	１１１
Ａ（３）＝５：	Ｗ３＝０００	０００	０００	０００	０００	１１１
Ａ（３）＝６：	Ｗ３＝０００	０００	０００	０００	０００	０００

を比較して分かるように、その性質上、複数の複製物から得られる相違部分は、必ず連続した要素Ｂとして得られることがわかる（したがって、結託攻撃による改ざんによって、この連続した部分に０と１が混在してくることになる）。

【００８４】そして、ある成分符号（ｉ）において、そのｄビット未満の数の１や０が孤立して存在する連続した部分の左端の位置と右端の位置、すなわちＡｍｉｎ（ｉ）とＡｍａｘ（ｉ）は、必ず、結託攻撃に用いられた複数の複製物のいずれかに埋め込まれた結託耐性符号の対応する成分符号の０と１の区切り目の位置（成分符号がすべて１の場合は、該成分符号の左端の位置、すべて０の場合は、該成分符号の右端の位置）すなわちＡｍｉｎ（ｉ）＝Ａｍａｘ（ｉ）に一致することがわかる。このような情報が、各成分符号Ｗ（ｉ）毎に得られる。それら情報Ａｍｉｎ（１）、Ａｍｉｎ（２）、…、Ａｍｉｎ（Ｍ）、Ａｍａｘ（１）、Ａｍａｘ（２）、…、Ａｍａｘ（Ｍ）を解析することによって、結託攻撃に使用された複製物に埋め込まれていたであろうユーザ識別符号すなわち結託耐性符号を特定し、該結託耐性符号に対応するユーザＩＤを、結託攻撃を行った結託者のユーザＩＤとして特定することができる。

【００８５】簡単な例としては、２人のユーザによる結託攻撃では、各成分符号ごとにおいて、Ａｍｉｎ（ｉ）は、２人のユーザの一方の持つ複製物に埋め込まれた符号のＡｍｉｎ（ｉ）＝Ａｍａｘ（ｉ）に一致し、Ａｍａｘ（ｉ）は、他方のユーザの持つ複製物に埋め込まれた符号のＡｍｉｎ（ｉ）＝Ａｍａｘ（ｉ）に一致する（各成分符号ごとに一方と他方の対応は異なりうる）。Ａｍｉｎ（１）とＡｍａｘ（１）からいずれか１つ、Ａｍｉｎ（２）とＡｍａｘ（２）からいずれか１つ、…Ａｍｉｎ（Ｍ）とＡｍａｘ（Ｍ）からいずれか１つを選択したものを、それぞれ、各成分符号の０と１の区切り目の位置として持つような結託耐性符号が存在すれば、それが求める解であり、該結託耐性符号に対応するユーザＩＤが結託者を示すことになる。

26

＊なる。

【００８２】さて、追跡アルゴリズムでは、検出された符号の各々の成分符号を調べ、予め定められたｄ（上記の例の場合、３）ビット未満の数の１や０が孤立して存在する成分符号が検出された場合に、結託攻撃がなされたものと判断することができる。また、この場合に、結託数が予め規定された許容数以下であったものと仮定して、上記の各々の成分符号Ｗ（ｉ）の第１の境界あるいは境界の最小値Ａｍｉｎ（ｉ）や第２の境界あるいは境界の最大値Ａｍａｘ（ｉ）に基づいて、結託攻撃に使用された複製物に埋め込まれていたであろう結託耐性符号を推定することができる。そして、結託耐性符号から、対応するユーザＩＤを求め、これを結託攻撃を行った結託者のユーザＩＤとして特定することができる。

【００８３】各々のＡ（ｉ）に対応する成分符号Ｍ（ｉ）は、例えば、先に例示したもの、すなわち、

000000　000000111111　000000111111111111

が埋め込まれており、ユーザＩＤ＝３のユーザが入手したコンテンツに、ユーザ識別符号として、

111111　000000000111　000000000111111111

が埋め込まれており、当該２人のユーザによって結託攻撃がなされ、次のようなユーザ識別符号、

010101　000000010111　000000101111111111

に改ざんされた場合に、この改ざん符号では、

Ａｍｉｎ（１）＝０、Ａｍａｘ（１）＝２
Ａｍｉｎ（２）＝２、Ａｍａｘ（１）＝３
Ａｍｉｎ（１）＝２、Ａｍａｘ（１）＝３

であり、図１０あるいは図１２を参照すると、Ａｍｉｎ（１）＝２、Ａｍａｘ（１）＝２、Ａｍａｘ（１）＝２

を、ユーザＩＤ＝２が満たし、かつ、Ａｍｉｎ（１）＝０、Ａｍａｘ（１）＝３、Ａｍａｘ（１）＝３を、ユーザＩＤ＝３が満たすので、この結託攻撃は、ユーザＩＤ＝２とユーザＩＤ＝３によって行われ、結託攻撃に用いられた符号は、

000000　000000111111　00000011111111111111

と、

111111　000000000111　00000000011111111111

であることを突き止めることができる。

【００８７】なお、３人以上のユーザによる結託攻撃では、これに用いられた全複製物に埋め込まれた結託耐性符号（ユーザ識別符号）の全成分符号が本来持つＡｍｉｎ（ｉ）＝Ａｍａｘ（ｉ）の全ては得られないことがあるが、ある複製物に埋め込まれた結託耐性符号の全てあるいはそのうちの多数の成分符号についてＡｍｉｎ（ｉ）＝Ａｍａｘ（ｉ）が得られたることが期待されるので、対象コンテンツから検出された符号から得られたＡｍｉｎ（１）、Ａｍｉｎ（２）、…、Ａｍｉｎ（Ｍ）、Ａｍａｘ（１）、Ａｍａｘ（２）、…、Ａｍａｘ（Ｍ）を適宜組み合わせて検証することによって、かりにすべての結託者のユーザＩＤが特定できなかったとしても、一部の結託者のユーザＩＤを特定することができる。

【００８８】さて、符号抽出部２１によって、検出対象となるコンテンツからユーザ識別符号（埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの）が抽出されると、電子透かし解析装置２の結託数推定部２２は、抽出された符号を解析することによって、結託攻撃に用いられたであろう複製物の結託数を推定する。

【００８９】以下では、電子透かし解析装置２の結託数推定部２２について説明する。

【００９０】（第１の構成例）まず、図３や図５に例示されるような、結託数推定部２２単独で（追跡アルゴリズム処理部２３の結果を利用することなしに）、結託攻撃に使用された複製物の個数を推定する場合（結託数推定部の第１の態様の場合）について説明する。なお、前述したように、結託耐性符号や追跡アルゴリズムは、基本的には、どのようなものでも適用可能である。また、結託攻撃がなされなかった場合を、結託攻撃に使用された複製物の個数＝１として扱うものとする。

【００９１】図１３に、この場合の結託数推定部２２の構成例を示す。図１３に示されるように、この結託数推定部２２は、抽出された符号（ユーザ識別符号）の各々の成分符号Ｗ（１）、Ｗ（２）、…、Ｗ（Ｍ）から、先に説明した、Ａｍｉｎ（１）、Ａｍｉｎ（２）、…、Ａｍｉｎ（Ｍ）のＭ個の第１グループのデータと、Ａｍａｘ（１）、Ａｍａｘ（２）、…、Ａｍａｘ（Ｍ）のＭ個の第２グループのデータの一方または両方を求める境界検出部２２１、求められた第１グループのデータと第２

グループのデータの一方または両方から統計的な量を求める統計処理部２２２、求められた統計的な量から結託数の推定値Ｃ0を求める推定結託数算出部２２３を含む。

【００９２】図１４に、概略的な手順の一例を示す。

【００９３】ここで、図１５に、結託攻撃において用いた複製物の個数（図１５ではｃと表す）を変えたときに、それに対応して、改ざん後の符号の各成文符号Ｗ（ｉ）から検出される第１の境界Ａｍｉｎ（ｉ）がどのような値をとるか、その確率を表す。なお、図１５では、Ａｍｉｎ（ｉ）が取りうる最大値（＝Ｎ（ｉ）－１）と最小値（＝０）との差（＝Ｎ（ｉ）の値）で除して正規化する。また、第１の境界Ａｍａｘ（ｉ）については、Ａｍｉｎ（ｉ）＝１－Ａｍａｘ（ｉ）の関係になる（図１５の横軸の０を１．０に、１．０を０に入れ替えたものになる）。

【００９４】これより分かるのは、第１の境界Ａｍｉｎについては、結託数ｃが大きくなると、Ａｍｉｎが小さな値をとる確率がより大きくなるように、バイアスされてくるということである。同様に、第２の境界Ａｍａｘについては、ｃが大きくなると、Ａｍａｘが大きな値をとる確率がより大きくなるように、バイアスされてくるということである。

【００９５】したがって、複数のＷ（ｉ）に対して、Ｍ個のＡｍｉｎ（ｉ）（またはＡｍａｘ（ｉ））の値をもとめ、それらＭ個のＡｍｉｎ（ｉ）（またはＡｍａｘ（ｉ））の分布を解析することによって、結託数ｃの値を統計的に推定することができることになる。

【００９６】統計処理部２２２および推定結託数算出部２２３による統計的な処理の方法には種々のバリエーションが考えられる。以下では、２つのバリエーションを説明する。

【００９７】（バリエーション１）まず、境界検出部２２１は、抽出された符号の各々の成分符号Ｗ（１）、Ｗ（２）、…、Ｗ（Ｍ）から、先に説明した、Ａｍｉｎ（１）、Ａｍｉｎ（２）、…、Ａｍｉｎ（Ｍ）のＭ個の第１グループのデータと、Ａｍａｘ（１）、Ａｍａｘ（２）、…、Ａｍａｘ（Ｍ）のＭ個の第２グループのデータの一方または両方を求める（ステップＳ１１）。

【００９８】次に、統計処理部２２２は、第１グループのデータＡｍｉｎ（ｉ）を利用する場合には、各Ｗ（ｉ）について、Ａｍｉｎ（１）、Ａｍｉｎ（２）、…、Ａｍｉｎ（Ｍ）の平均＜Ａｍｉｎ＞を求める（ステップＳ１２）。ただし、それらの値が取りうる最大値と最小値との差（＝対応するＮ（ｉ）の値）で除して正規化する。すなわち、Ｗ（ｉ）、Ｎ（ｉ）、Ａ（ｉ）についての第１グループのデータの平均（第１の平均）＜Ａｍｉｎ＞は、

＜Ａｍｉｎ＞＝｜Ａｍｉｎ（１）／Ｎ（１）＋Ａｍｉｎ（２）／Ｎ（２）＋…＋Ａｍｉｎ（Ｍ）／Ｎ（Ｍ）｜／

M
である。

【００９９】また、第２グループのデータＡｍａｘ（ｉ）を利用する場合には、統計処理部２２２は、各Ｗ（ｉ）、Ｎ（ｉ）、Ａ（ｉ）についての第２グループのデータの平均（第２の平均）＜Ａｍａｘ＞を求める（ステップＳ１２）。＜Ａｍａｘ＞は、

＜Ａｍａｘ＞＝｛Ａｍａｘ（１）／Ｎ（１）＋Ａｍａｘ（２）／Ｎ（２）＋…＋Ａｍａｘ（Ｍ））／Ｎ（Ｍ）｝／Ｍ

である。

【０１００】第１グループのデータＡｍｉｎ（ｉ）および第２グループのデータＡｍａｘ（ｉ）を利用する場合には、＜Ａｍｉｎ＞および＜Ａｍａｘ＞を求める（ステップＳ１２）。

【０１０１】次に、推定結託数算出部２２３は、後述するような方法によって、＜Ａｍｉｎ＞や＜Ａｍａｘ＞から、結託数の推定値Ｃ０を求める（ステップＳ１３）。

【０１０２】以下、結託数の推定値Ｃ０を求める方法について説明する。

【０１０３】ここで、Ｃ０人の結託者による結託攻撃が行われたとする。

【０１０４】前述したように、このＣ０が、結託耐性符号の想定している結託数の上限ｃを越えているか否かを知ることによって、例えば、追跡アルゴリズムが出力した結託者のユーザＩＤが正しいものであるか、それとも無実のユーザのものであるかに関する判断の材料となる。

【０１０５】前述したように、各成分符号Ｗ（ｉ）において、結託語の符号後を復号することによって、ＡｍｉｎやＡｍａｘを検出することができ（それらは、いずれかの結託者の結託前の符号語の対応する成分符号ＷのＡｍｉｎ＝Ａｍａｘである）、それらに対して統計的な処理を行うことでＣ０を推定することができる。統計的な処理の方法は様々あるが、ここでは、各成分符号Ｗ（ｉ）についてのＡｍｉｎ（ｉ）の平均＜Ａｍｉｎ＞からＣ０を推定する方法について説明する。

【０１０６】ある成分符号Ｗ（ｉ）について、各結託者に割り当てられている整数Ａ（ｉ）が０からＮ（ｉ）－１までの整数のいずれかをとる確率は、０からＮ（ｉ）－１までの整数のいずれについても等しく、１／Ｎ（ｉ）で与えられるとすると、Ａｍｉｎ（ｉ）がある値ｘをとる確率Ｐｒ［Ａｍｉｎ（ｉ）＝ｘ］は、結託者の数がＣ０のとき、次式で与えられる。

【０１０７】

【数１】

$$Pr[A\ min(i) = x] = \left(1 - \frac{x}{N_{(i)}}\right)^{C_0} - \left(1 - \frac{x+1}{N_{(i)}}\right)^{C_0}$$

ここで、ｘは、０からＮ（ｉ）－１までの整数に値をとる。

【０１０８】そこで、実際に復号によって得られた各々の成分符号Ｗ（ｉ）についてのＡｍｉｎ（ｉ）を、それぞれ、それらの値が取りうる最大値と最小値との差すなわちＮ（ｉ）の値で除して正規化し（Ａｍｉｎ（ｉ）／Ｎ（ｉ））、Ｍ個のＡｍｉｎ（ｉ）／Ｎ（ｉ）の平均＜Ａｍｉｎ＞、すなわち、

＜Ａｍｉｎ＞＝｛Ａｍｉｎ（１）／Ｎ（１）＋Ａｍｉｎ（２）／Ｎ（２）＋…＋Ａｍｉｎ（Ｍ）／Ｎ（Ｍ）｝／Ｍ

を求める。

【０１０９】＜Ａｍｉｎ＞は、ｙ＝ｘ／Ｎ（ｉ）を０から１の間の実数として連続近似することによって、次のような期待値＜ｙ＞で近似できる。

【０１１０】

【数２】

$$\langle y \rangle = \int_0^1 dy\, y P[y] = c_0 \int_0^1 dy\, y(1-y)^{c_0 - 1} = \frac{1}{c_0 + 1}$$

【０１１１】ここで、Ｐ［ｙ］は、Ｐｒ［Ａｍｉｎ（ｉ）＝ｘ］に対するＮ（ｉ）→∞の連続極限によって与えられ、次式で表される。

【０１１２】

【数３】

$$P[y] = \lim_{N_{(i)} \to \infty} N_{(i)} Pr[\min = N_{(i)} y] = c_0 (1-y)^{c_0 - 1}$$

【０１１３】よって、＜Ａｍｉｎ＞＝＜ｙ＞の近似より、Ｃ０＝＜Ａｍｉｎ＞$^{-1}$－１となり、結託数Ｃ０が推定できる。

【０１１４】＜Ａｍａｘ＞を用いた場合にも、同様にして、Ｃ０＝（１－＜Ａｍａｘ＞）$^{-1}$－１となり、結託数Ｃ０が推定できる。

【０１１５】また、＜Ａｍｉｎ＞および＜Ａｍａｘ＞を用いて、Ｃ０＝（１／２＋＜Ａｍｉｎ＞／２－＜Ａｍａｘ＞／２）$^{-1}$－１として、結託数Ｃ０を推定することもできる。

【０１１６】したがって、第１グループのデータＡｍｉｎ（ｉ）のみを利用する場合には、推定結託数算出部２２３は、上記のような方法によって、＜Ａｍｉｎ＞から、結託数の推定値Ｃ０を求めることができる。

【０１１７】また、第２グループのデータＡｍａｘ（ｉ）のみを利用する場合には、推定結託数算出部２２３は、上記のような方法によって、＜Ａｍａｘ＞から、結託数の推定値Ｃ０を求めることができる。

【０１１８】また、第１グループのデータＡｍｉｎ（ｉ）および第２のグループのデータＡｍａｘ（ｉ）を利用する場合には、推定結託数算出部２２３は、上記のような方法によって、＜Ａｍｉｎ＞および＜Ａｍａｘ＞から、結託数の推定値Ｃ０を求める。

31

【０１１９】なお、第１グループのデータＡｍｉｎ（ｉ）および第２のグループのデータＡｍａｘ（ｉ）を利用する場合には、推定結託数算出部２２３は、＜Ａｍｉｎ＞から、結託数の推定値Ｃ０（Ｃｍｉｎとする）を求めるとともに、＜Ａｍａｘ＞から、結託数の推定値Ｃ０（Ｃｍａｘとする）を求め、ＣｍｉｎとＣｍａｘを列記して出力するか、またはＣｍｉｎとＣｍａｘのうちの最大値を出力するか、またはＣｍｉｎとＣｍａｘの平均を出力することも可能である（その他のバリエーションも可能である）。

【０１２０】ここで、具体例を示す。ここでは、Ｍ＝２

Ｗ(1)	：	Ｎ(1)＝５１２、Ａｍｉｎ＝　１３、Ａｍａｘ＝４９７
Ｗ(2)	：	Ｎ(2)＝５１３、Ａｍｉｎ＝　４６、Ａｍａｘ＝５０５
Ｗ(3)	：	Ｎ(3)＝５１５、Ａｍｉｎ＝　１６、Ａｍａｘ＝５００
Ｗ(4)	：	Ｎ(4)＝５１７、Ａｍｉｎ＝　　７、Ａｍａｘ＝５０７
Ｗ(5)	：	Ｎ(5)＝５２１、Ａｍｉｎ＝　１９、Ａｍａｘ＝５１９
Ｗ(6)	：	Ｎ(6)＝５２３、Ａｍｉｎ＝　２４、Ａｍａｘ＝４５１
Ｗ(7)	：	Ｎ(7)＝５２７、Ａｍｉｎ＝１２３、Ａｍａｘ＝４７４
Ｗ(8)	：	Ｎ(8)＝５２９、Ａｍｉｎ＝　５４、Ａｍａｘ＝５２４
Ｗ(9)	：	Ｎ(9)＝５３３、Ａｍｉｎ＝　１９、Ａｍａｘ＝４７８
Ｗ(10)	：	Ｎ(10)＝５４１、Ａｍｉｎ＝　　４、Ａｍａｘ＝５３０
：	：	：　　、　　：　　、　　：
Ｗ(247)	：	Ｎ(257)＝２２３９、Ａｍｉｎ＝　３１、Ａｍａｘ＝２１７２
Ｗ(248)	：	Ｎ(248)＝２２４３、Ａｍｉｎ＝２２９、Ａｍａｘ＝２１４２
Ｗ(249)	：	Ｎ(249)＝２２５１、Ａｍｉｎ＝１９７、Ａｍａｘ＝２０２９
Ｗ(250)	：	Ｎ(250)＝２２６７、Ａｍｉｎ＝１３３、Ａｍａｘ＝２１６７
Ｗ(251)	：	Ｎ(251)＝２２６９、Ａｍｉｎ＝１２５、Ａｍａｘ＝２０３３
Ｗ(252)	：	Ｎ(252)＝２２７３、Ａｍｉｎ＝　８４、Ａｍａｘ＝２２６０
Ｗ(253)	：	Ｎ(253)＝２２８１、Ａｍｉｎ＝　５５、Ａｍａｘ＝２１９２
Ｗ(254)	：	Ｎ(254)＝２２８７、Ａｍｉｎ＝　５３、Ａｍａｘ＝２１６４
Ｗ(255)	：	Ｎ(255)＝２２９３、Ａｍｉｎ＝　２９、Ａｍａｘ＝２２０９
Ｗ(256)	：	Ｎ(256)＝２２９７、Ａｍｉｎ＝　１３、Ａｍａｘ＝２２０７

また、２５６個のＡｍｉｎから＜Ａｍｉｎ＞を計算すると、

＜Ａｍｉｎ＞＝０．０６１８７１

が得られ、これを、Ｃ０＝＜Ａｍｉｎ＞$^{-1}-1$に代入することによって、

Ｃ０＝１５．１６３（人）

となり、真の結託者の数に近い値が得られた。

【０１２１】また、＜Ａｍａｘ＞＝０．９３５３８が得られ、これを、Ｃ０＝（１－＜Ａｍａｘ＞）$^{-1}-1$に代入することによって、

Ｃ０＝１４．４７５（人）

となり、真の結託者の数に近い値が得られていることがわかる。

【０１２２】また、Ｃ０＝（１／２＋＜Ａｍｉｎ＞／２－＜Ａｍａｘ＞／２）$^{-1}-1$を用いると、

Ｃ０＝１４．８１１（人）

となり、真の結託者の数に近い値が得られていることがわかる。

【０１２３】同様の条件で、ある３２人の結託攻撃を行った場合における、結託数の推定結果の一例は、次のようになった。

＜Ａｍｉｎ＞＝０．０２９０６５

＜Ａｍａｘ＞＝０．９６６８４３

Ｃ０＝＜Ａｍｉｎ＞$^{-1}-1$＝３３．４０６

Ｃ０＝（１－＜Ａｍａｘ＞）$^{-1}-1$＝２９．１６０

Ｃ０＝(1/2+<Amin>/2-<Amax>/2)$^{-1}-1$＝３１．１４３

同様の条件で、ある４８人の結託攻撃を行った場合における、結託数の推定結果の一例は、次のようになった。

＜Ａｍｉｎ＞＝０．０１９８８４

＜Ａｍａｘ＞＝０．９７７３８２

Ｃ０＝＜Ａｍｉｎ＞$^{-1}-1$＝４９．２９２

Ｃ０＝（１－＜Ａｍａｘ＞）$^{-1}-1$＝４３．２１３

Ｃ０＝(1/2+<Amin>/2-<Amax>/2)$^{-1}-1$＝４６．０５７

（バリエーション２）次に、他のバリエーションを説明する。

【０１２４】ここでは、バリエーション１との相違点を説明する。バリエーション１では、統計処理部２２２は、Ａｍｉｎ（ｉ）の平均やＡｍａｘ（ｉ）の平均を求

32

＊５６、Ｎ（１）＝５１２、Ｎ（２５６）＝２２９７、Ｎ（２）～Ｎ（２５５）は５１３から２２９３の間の値とし、ｄ＝３０のΓ０(ｎ，ｄ)符号を用いることとして、ある１６人で結託攻撃を行った場合に、結託攻撃後のコンテンツから検出した符号（ユーザ識別符号）をもとに、２５６個の成分符号Ｗ（１）～Ｗ（２５６）について、Ａｍｉｎ（１）、Ａｍａｘ（１）、Ａｍｉｎ（２）、Ａｍａｘ（２）、…、Ａｍｉｎ（２５６）／Ａｍａｘ（２５６）を求めた一例において、その一部を抜粋して示すと、次のようになった。

め、推定結託数算出部２２３は、Ａｍｉｎ（ｉ）の平均やＡｍａｘ（ｉ）の平均から、結託者の数ｃ0を推定した。

【０１２５】バリエーション２では、統計処理部２２２は、Ａｍｉｎ（ｉ）やＡｍａｘ（ｉ）から、他の統計量を求め、推定結託数算出部２２３は、該他の統計量から、結託者の数ｃ0を推定する。

【０１２６】例えば、図１５をみると、Ａｍｉｎ（ｉ）については、結託数ｃが大きくなるほど、横軸におけるある値Ａｔｈを基準値として、基準値Ａｔｈ以下の値を持つＡｍｉｎ（ｉ）の数を、基準値Ａｔｈを越える値を持つＡｍｉｎ（ｉ）の数で割った比αが大きくなることがわかる。一方、Ａｍａｘ（ｉ）については、結託数ｃが大きくなるほど、比αが小さくなる。

【０１２７】そこで、例えば先の例のように、ある成分符号Ｗ（ｉ）について、各結託者に割り当てられている整数Ａ（ｉ）が０からＮ（ｉ）－１までの整数のいずれかをとる確率は、０からＮ（ｉ）－１までの整数のいずれについても等しく、１／Ｎ（ｉ）で与えられるとして、予め、結託数ｃのときの、基準値Ａｔｈ以下の値を持つＡｍｉｎ（ｉ）の数を、基準値Ａｔｈを越える値を持つＡｍｉｎ（ｉ）の数で割った比αを与える関数ｆ（ｃ）＝αの逆関数ｃ＝f^{-1}（α）を予め求めておく。

【０１２８】そして、統計処理部２２２は、Ａｍｉｎ（ｉ）から、比αを求め（ステップＳ１２）、推定結託数算出部２２３は、比αを、上記のｃ＝f^{-1}（α）に代入して、結託数ｃを推定することができる（ステップＳ１３）。Ａｍａｘ（ｉ）についても同様である。もちろん、Ａｍｉｎ（ｉ）とＡｍａｘ（ｉ）の一方を用いてもよいし、両方を用いてもよい。

【０１２９】なお、上記では、結託数の値を推定するようにしたが、結託数を何段階かのレベルで求めるようにしてもよい。例えば、Ａｍｉｎ（ｉ）について求めた上記の比αが予め定められた基準値以下の場合には、結託数が少ない（あるいは許容数以下）を示す情報を出力し、予め定められた基準値を越える場合には、結託数が多い（あるいは許容数を超過）を示す情報を出力する関数を用いるようにしてもよい。

【０１３０】また、これまで説明した以外のバリエーションも可能である。

【０１３１】（第２の構成例）次に、図４に例示されるような、追跡アルゴリズム処理部２３の結果を利用して、結託攻撃に使用された複製物の個数を推定する場合（結託数推定部の第２の態様の場合）について説明する。なお、前述したように、結託耐性符号や追跡アルゴリズムは、基本的には、どのようなものでも適用可能である。また、結託攻撃がなされなかった場合を、結託攻撃に使用された複製物の個数＝１として扱うものとする。

【０１３２】図１６に、この場合の結託数推定部２２の

構成例を示す。図１６に示されるように、この結託数推定部２２は、追跡アルゴリズム処理部２３から結託者の全部または一部のユーザＩＤが出力された場合に、該ユーザＩＤを後述する弱ＩＤ（弱識別情報）と非弱ＩＤ（非弱識別情報）とに分類する弱ＩＤ・非弱ＩＤ分類部２４１、この分類結果を基に、弱ＩＤの数と非弱ＩＤの数とに基づく統計的な量を求める統計処理部２４２、求められた統計的な量から結託数の推定値Ｃ0を求める推定結託数算出部２４３を含む。なお、統計処理部２４２および推定結託数算出部２４３による統計的な処理の方法には種々のバリエーションが考えられる。

【０１３３】図１７に、概略的な手順の一例を示す。

【０１３４】なお、この場合には、電子透かし埋込装置１（の符号生成部１１）は、弱ＩＤをユーザＩＤとして用いないものとする。

【０１３５】以下では、第１の構成例との相違点を中心に説明する。

【０１３６】ここで、弱ＩＤと非弱ＩＤについて説明する。

【０１３７】弱ＩＤとは、ユーザＩＤとして用いた場合に、結託攻撃を行っていないユーザのユーザＩＤであるにもかかわらず、結託者のユーザＩＤとして誤検出される可能性のより高いユーザＩＤである（誤検出に弱いＩＤという意味から、このように呼ぶ）。非弱ＩＤとは、ユーザＩＤ候補のうちから、弱ＩＤを除いたユーザＩＤであり、非弱ＩＤのみがユーザＩＤとして使用される。

【０１３８】非弱ＩＤは、所定の判定アルゴリズムによって判定する方法と、誤検出される可能性のより高いユーザＩＤを何らかの指針（例えば、対応する結託耐性符号の成分符号の全部または多数について、その正規化したＡｍｉｎ＝Ａｍａｘが０または１に近い等）によって予め決めてしまう方法とがある。

【０１３９】ここで、図１８に示すフローチャートを用いて、図７の符号生成部１１の場合に、与えられたユーザＩＤ（の候補）が弱ＩＤか非弱ＩＤかを判定する処理手順の一例について説明する。

【０１４０】まず、対象となったユーザＩＤを一つずつシーケンシャルに入力し(ステップＳ３１)、このユーザＩＤが結託者ＩＤとして誤検出される確率(誤検出確率)を推定する(ステップＳ３２)。この誤検出確率の推定は、例えば前述したp_i（＝Ｎ（ｉ））、ｋ、ｋ′（＝Ｍ），結託者総数の最大値ｃ、ユーザ総数ｎ、ｚといったパラメータを用いて次のようにして行われる。なお、ｋについては、図７の法記憶部１２１－１，１２１－２，…，１２１－ｋ′で用意されているｋ′個の素数ｐ１（＝Ｎ（１）），ｐ２（＝Ｎ（２）），…，ｐｋ′（＝Ｎ（ｋ′））から任意のｋ個の素数を選んだとき、それらのｋ個の素数の積をｎ以上とするものである（例えば、この積はｎ≦Ｎ（１）×Ｎ（２）×…×Ｎ（ｋ）である）。また、ｚは、１以上の正整数であり、例え

35

ば、k′＝c(k＋z)／２を満足する正整数である。

【０１４１】まず、次式を定義する。

$$Pr[x; p, c] = \begin{cases} \left(1 - \frac{x}{p}\right)^c - \left(1 - \frac{x+1}{p}\right)^c & \text{for } x \neq p-1 \\ \left(\frac{1}{p}\right)^c & \text{for } x = p-1 \end{cases}$$

次に、次式を定義する。

【０１４３】

【数５】

$$Q[x; p, c] = Pr[x; p, c] + Pr[p-1-x; p, c]$$

【０１４４】あるユーザＩＤ(＝ｕとする)が結託者ＩＤ※

36

*【０１４２】

*【数４】

※として誤検出される確率を概ね表す量として、次式で表される評価値ＥＥＰを計算する。

【０１４５】

【数６】

$$EEP = 1 - \prod_{\{j(1), j(2), \ldots, j(k+z)\} \subset \{1,2,\ldots,k'\}, j(1)<j(2)<\ldots j(k+z)} \left\{1 - \prod_{j=1,2\ldots,k+z} Q[u_{pi}; p_i, c]\right\}$$

【０１４６】ここで、u_p＝ｕ mod ｐとする。これ以外にも、ある利用者ＩＤについて誤検出確率を近似する評価値が存在するならば、それを該評価値ＥＥＰの代わりに用いることが可能である。例えば、次式で表される評価値ＥＥＰを用いてもよい。

【０１４７】

【数７】

$$EEP = \sum_{i=1,2,\ldots,k'} Q[u_{pi}; p_i, c]$$

【０１４８】次に、ステップＳ３２で推定された誤検出確率(例えば、該ＥＥＰ)が所定の閾値を超えたか否かを調べ(ステップＳ３３)、閾値を超える場合は、ユーザＩＤ（の候補）が弱ＩＤであると判定し(ステップＳ３４)、また誤検出確率が閾値以下の場合は、ユーザＩＤ（の候補）が非弱ＩＤであると判定する(ステップＳ３５)。

【０１４９】さて、結託攻撃を行った結託数ｃが大きくなると、追跡アルゴリズムが当該結託攻撃を受けたコンテンツから結託者のユーザＩＤを推定した場合に、得られる結果として弱ＩＤが増加してくる。したがって、弱ＩＤの数と非弱ＩＤの数との比βを評価することで、その比βを生み出す結託数ｃの値が推定できる。

【０１５０】すなわち、結託数ｃが大きくなるほど、弱ＩＤの数を、非弱ＩＤの数で割った比βが大きくなるので、予め、結託数ｃのときの比βを与える関数ｈ（ｃ）＝βの逆関数ｃ＝h^{-1}（β）を予め求めておくことで、比βから結託数ｃを推定することができる。

【０１５１】まず、弱ＩＤ・非弱ＩＤ分類部２４１は、追跡アルゴリズム処理部２３から結託者の全部または一部のユーザＩＤが出力された場合に、該ユーザＩＤを、弱ＩＤと非弱ＩＤとに分類する（ステップＳ２１）。なお、弱ＩＤか非弱ＩＤかの判断は、例えば、弱ＩＤのリストを記憶しておき、与えられたユーザＩＤが該リストに登録されているものと一致するか否かを調べることによって、一致すれば弱ＩＤと判断し、一致しなければ非弱ＩＤと判断するようにしてもよいし、ユーザＩＤが弱ＩＤか非弱ＩＤかを判定する手順が作成可能であれば、該判断手順によって弱ＩＤか非弱ＩＤかを判断するようにしてもよい。

【０１５２】次に、統計処理部２２２は、分類された弱ＩＤと非弱ＩＤとに基づいて、弱ＩＤの数を非弱ＩＤの数で割った比βを求める（ステップＳ２２）。

【０１５３】そして、推定結託数算出部２２３は、比βを、上記のｃ＝h^{-1}（β）に代入して、結託数ｃを推定することができる（ステップＳ２３）。

【０１５４】なお、上記では、結託数の値を推定するようにしたが、結託数を何段階かのレベルで求めるようにしてもよい。例えば、求めた上記の比βが予め定められた基準値以下の場合には、結託数が少ない（あるいは許容数以下）を示す情報を出力し、予め定められた基準値を越える場合には、結託数が多い（あるいは許容数を超過）を示す情報を出力する関数を用いるようにしてもよい。

【０１５５】なお、以上では、コンテンツの複製物に、ユーザＩＤに対応する符号を埋め込むようにしたが、その代わりに、複製物の複製物ＩＤとそのユーザを特定するための情報（例えば、ユーザ名、あるいはユーザＩＤ等）との対応を保存または復元可能にしておき、コンテンツの複製物に、複製物ＩＤに対応する符号を埋め込むようにしてもよい。

【０１５６】以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【０１５７】本実施形態の電子透かし解析装置は、ハードウェアとしても、ソフトウェア（（コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラム）としても、実現可能である。また、電子透かし解析装置を

ソフトウェアで実現する場合には、記録媒体によってプログラムを受け渡しすることも、通信媒体によってプログラムを受け渡しすることもできる。もちろん、それらは、電子透かし埋込装置についても同様である。また、電子透かし埋込装置や電子透かし解析装置をハードウェアとして構成する場合、半導体装置として形成することができる。また、本発明を適用した電子透かし解析装置を構成する場合、あるいは電子透かし解析プログラムを作成する場合に、同一構成を有するブロックもしくはモジュールがあっても、それらをすべて個別に作成することも可能であるが、同一構成を有するブロックもしくはモジュールについては１または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。電子透かし埋込装置を構成する場合、あるいは電子透かし埋め込みプログラムを作成する場合も、同様である。また、電子透かし埋込装置および電子透かし解析装置を含むシステムを構成する場合、あるいは電子透かし埋め込みプログラムおよび電子透かし検出プログラムを含むシステムを作成する場合には、電子透かし埋込装置（あるいはプログラム）と電子透かし解析装置（あるいはプログラム）に渡って、同一構成を有するブロックもしくはモジュールについては１または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【０１５８】また、電子透かし埋込装置や電子透かし解析装置をソフトウェアで構成する場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【０１５９】ところで、デジタル透かしに対する透かし技術は、デジタルデータの他に、ある情報あるいは物質の一部の内容を変更しても、その情報あるいは物質の同一性、同質性あるいは経済的価値等を変じないようなものにも適用可能であり、本発明は、デジタルデータの他に、そのような情報あるいは物質にも適用可能である。

【０１６０】例えば、本発明において、結託攻撃への耐性を持つ電子透かし埋込装置／電子透かし解析装置において用いられる、埋め込まれる符号の生成手段、検出手段は、化学的に合成される、あるいは、工業的に管理された環境下で生物的に生成される化合物あるいは化学物質の出所の追跡にも応用できる。化合物としては、ＤＮＡ、ＲＮＡ、タンパク質、その他の高分子の化合物が、符号を埋め込むことができる冗長性を多く持つ。

【０１６１】以下では、本発明を、化合物の複製物に対して個別の識別情報（ユーザＩＤ、製造者ＩＤ、販売者ＩＤ、取引ＩＤ、それらを組み合わせた情報など）を埋め込み、その出所を特定する手段を与える透かし技術として適用する場合について説明する。

【０１６２】化合物は、複数の原子、分子、基といった物質から構成されている。例えば、ＤＮＡやＲＮＡは、所定のアミノ酸の配列構造を持っており、別のアミノ酸

で置きかえるか如何かによって情報が表現されているとみなせる。その構造の中には、（デジタルコンテンツの場合には、データを変更しても、作品の同一性あるいは経済的価値を変えない場合があるのと同様に、）化合物の場合には、組成を変更しても、当該目的において、その作用・副作用・効用等の性質・機能等（別の観点でみれば、経済的価値）を変えない場合がある。

【０１６３】そのような許容された範囲内の変更によって、その複製物を個々に識別する情報を埋め込むことができる。

【０１６４】本発明の電子透かしを化合物に適用する場合、化合物に対する透かし埋込装置は、デジタルコンテンツに対する透かし埋込装置におけるデジタルコンテンツの所定の部分のビットを変更する構成を、化合物の所定の部分の組成を変更する装置に置き換えたものである。また、化合物に対する透かし解析装置は、デジタルコンテンツに対する透かし解析装置において透かし情報を検出するためにデジタルコンテンツの所定の部分のビットの値を読み取る情報を検出する構成を、透かし情報を検出するために化合物の所定の部分の組成を解析する装置に置き換えたものである。すなわち、化合物とのインタフェースとなる装置が相違するだけで、原理的には、デジタルコンテンツに対する透かし技術と同じである。

【０１６５】図１９に、化合物に対する透かし埋込装置の構成例を示す。

【０１６６】符号生成部１００１は、その化合物に埋め込むべき識別情報を入力とし、結託耐性符号を生成する。

【０１６７】特定部位の構造変換部１００２～１００４は、それぞれ、結託耐性符号の各ビット、あるいは、ビットの各集合に対して、その値に応じて化合物の構造を変換するものである。特定部位の構造変換部１００２は、原化合物の特定部位１を処理し、特定部位の構造変換部１００３は、特定部位１を処理済みの化合物の特定部位２を処理し、特定部位の構造変換部１００４は、特定部位１，２を処理済みの化合物の特定部位３を処理して、所望する埋込済み化合物を生成する。もちろん、図１９では、３つの構造変換部が示されているが、その数は３に限定されるものではない。

【０１６８】ここで、化合物の構造の変換とは、その化合物の利用の目的に適した性質あるいは機能等を損なわず且つ新たな弊害あるいは副作用等をもたらさないままで、異なる構造を持つ化合物に変換する手段のことである。あるいは、その化合物が純粋な化合物ではなく、混合物である場合には、その組成を変更する手段であってもよい。

【０１６９】図２０に、化合物に対する透かし埋込装置の他の構成例を示す。

【０１７０】図１９の構成例は、すでに合成された化合

物の構造を後から変換するものであったっが、図２０の構成例は、化合物の合成時に符号を埋め込むものである。

【０１７１】符号生成部１０１１は、その化合物に埋め込むべき識別情報を入力とし、結託耐性符号を生成する。

【０１７２】この場合、各合成材料毎に、結託耐性符号の各ビット、あるいは、ビットの各集合に対して、その値に応じた合成材料が容易されており、合成材料部１０１２～１０１４は、それぞれ、結託耐性符号の各ビット、あるいは、ビットの各集合に対して、その値に応じた化合物の合成材料を選択するものである。もちろん、図２０では、３つの合成材料選択部が示されているが、その数は3に限定されるものではない。

【０１７３】合成部１０１５は、各合成材料部１０１２～１０１４により選択された合成材料を合成して、所望する埋込済み化合物を生成する。

【０１７４】さて、化合物に対する結託攻撃では、基本的にはデジタルコンテンツに対する結託攻撃と同様で、例えば、複数の異なる識別情報（例えば、ユーザＩＤ、製造者ＩＤ、ユーザＩＤ及び製造者ＩＤ等）が埋め込まれた化合物の構造を比較することで、差異のある部分の構造を改変することで作られる。

【０１７５】図２１に、化合物に対する透かし解析装置の構成例を示す。

【０１７６】特定部位の構造読み取り部１２０１～１２０１は、図１９の特定部位の構造変換部１００２～１００４あるいは図２０の合成材料部１０１２～１０１４に対応するもので、その化合物中の特定部位の構造を読み取り、それをビットあるいはビットの集合である情報として出力する。

【０１７７】符号復号部１２０４は、それらのビットから追跡すべき符号語を再現し、結託数を推定するもので、デジタルコンテンツに対する電子透かし解析装置２の持つ、ビットから追跡すべき符号語を再現し、結託数を推定する機能と同様である。

【０１７８】もちろん、化合物に対する透かし解析装置は、必要に応じて、追跡アルゴリズムの機能を持つものである。

【０１７９】また、化合物に対する透かし解析装置は、結託数を推定する機能を持たず、追跡アルゴリズムの機能を持つ構成も可能である。

【０１８０】ここで、本発明に用いられる化合物の構造の変換手段や構造の読み取り手段について、利用可能な技術を例示する。以下では、ＤＮＡの場合を例にとって説明する。

【０１８１】ＤＮＡにおいて、その塩基配列を求めることを、シークエンシングという。シークエンシングの方法としては、ショットガン法、プライマーウォーク法、ネスティッドデレーション法などが知られている。これ

らは、いずれも遺伝子のクローニングによる方法である。シークエンシングで用いる試薬・機器・装置の例については、各種の方法が提案されている。例えば、渡辺格監修、杉浦昌弘編集「クローニングとシークエンス」、農村文化社（１９８９年）や、榊佳之等編「ゲノムサイエンス」、共立出版（１９９９年）などに開示されている。

【０１８２】同様に、ＤＮＡの例では、新しい遺伝子を導入する際に用いられている遺伝子導入法により構造変換が可能である。遺伝子導入法には、燐酸カルシウム沈殿法、デキストラン法、リボフェクション法などの化学的な方法や、電気穿孔法、マイクロインジェクション法などが知られている。例えば、波賀信幸著「分子細胞工学」、コロナ社（２０００年）に開示されている。

【０１８３】なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。また、この発明の実施の形態は、個別装置としての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【０１８４】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１８５】

【発明の効果】本発明によれば、結託耐性符号の埋め込まれたデジタルコンテンツの複製物から検出した符号についての統計的な手法に基づく推定を行うことによって、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る電子透かし埋込装置及び電子透かし解析装置を含むコンテンツ流通システムの概略構成を示す図

【図２】同実施形態に係る電子透かし埋込装置の構成例を示す図

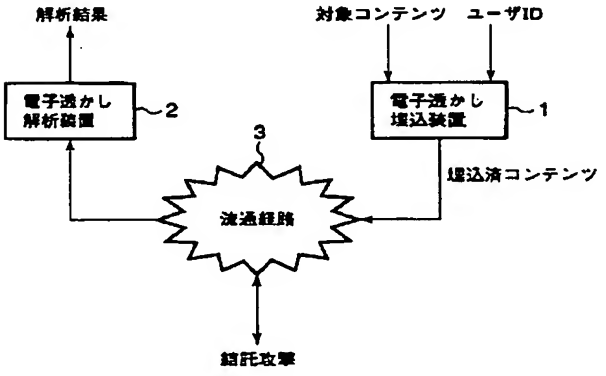
41

【図３】同実施形態に係る電子透かし解析装置の構成例を示す図
【図４】同実施形態に係る電子透かし解析装置の他の構成例を示す図
【図５】同実施形態に係る電子透かし解析装置のさらに他の構成例を示す図
【図６】同実施形態に係る電子透かし埋込装置の概略的な手順の一例を示すフローチャート
【図７】同実施形態に係る電子透かし埋込装置の符号生成部の構成例を示す図
【図８】図７の符号生成部の成分符号生成部の構成例を示す図
【図９】同実施形態に係る電子透かし埋込装置により生成される成分符号の例について説明するための図
【図１０】同実施形態における各ユーザＩＤに対応する複数の整数の組の例について説明するための図
【図１１】同実施形態における各ユーザＩＤに対応する結託耐性符号の例について説明するための図
【図１２】同実施形態における各成分符号でのビットパターンに関する境界の位置について説明するための図
【図１３】同実施形態に係る電子透かし解析装置の結託数推定部の構成例を示す図
【図１４】同実施形態に係る電子透かし解析装置の結託数推定部の概略的な手順の一例を示すフローチャート
【図１５】結託攻撃において用いる複製物の個数と、改ざんされた結託耐性符号の各成分符号において検出されるビットパターンに関する境界の位置との関係について説明するための図
【図１６】同実施形態に係る電子透かし解析装置の結託数推定部の他の構成例を示す図
【図１７】同実施形態に係る電子透かし解析装置の結託数推定部の概略的な手順の他の例を示すフローチャート
【図１８】同実施形態においてユーザＩＤが弱ＩＤか非弱ＩＤかを判定するための手順の一例を示すフローチャート
【図１９】同実施形態に係る化合物に対する透かし埋込＊

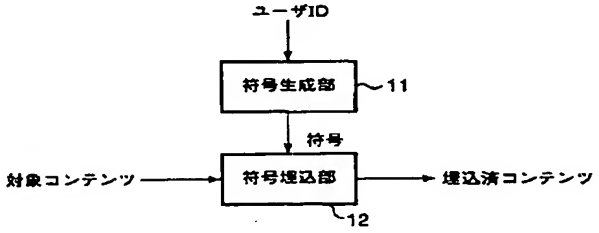
42

＊装置の構成例を示す図
【図２０】同実施形態に係る化合物に対する透かし埋込装置の他の構成例を示す図
【図２１】同実施形態に係る化合物に対する透かし解析装置の他の構成例を示す図
【符号の説明】
１…電子透かし埋込装置
２…電子透かし解析装置
３…流通経路
１１…符号生成部
１２…符号埋込部
２１…符号抽出部
２２…結託数推定部
２３…追跡アルゴリズム処理部
１２１－１～１２１－ｋ′…法記憶部
１２２－１～１２２－ｋ′…剰余計算部
１２３…符号パラメータ記憶部
１２４－１～１２４－ｋ′…成分符号生成部
１２５…符号連接部
１３１…減算部
１３２…“０”列生成部
１３３…“１”列生成部
３４…連接部
２２１…境界検出部
２２２…統計処理部
２２３…推定結託数算出部
２４１…弱ＩＤ・非弱ＩＤ分類部
２４２…統計処理部
２４３…推定結託数算出部
１００１，１０１１…符号生成部
１００２～１００４…特定部位の構造変換部
１０１２～１０１４…合成材料部
１０１５…合成部
１２０１～１２０１…特定部位の構造読み取り部
１２０４…符号復号部

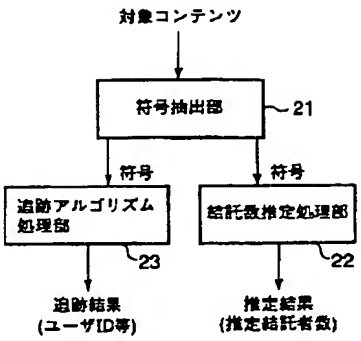
【図１】



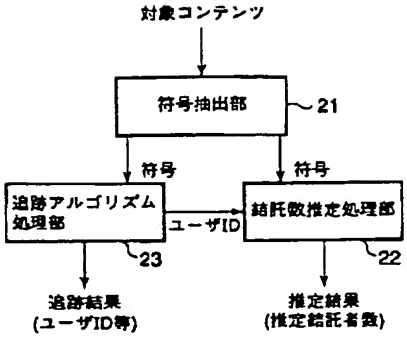
【図２】



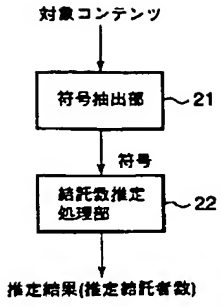
【図３】



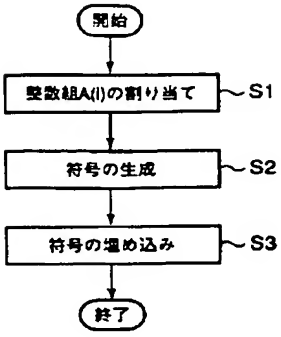
【図４】



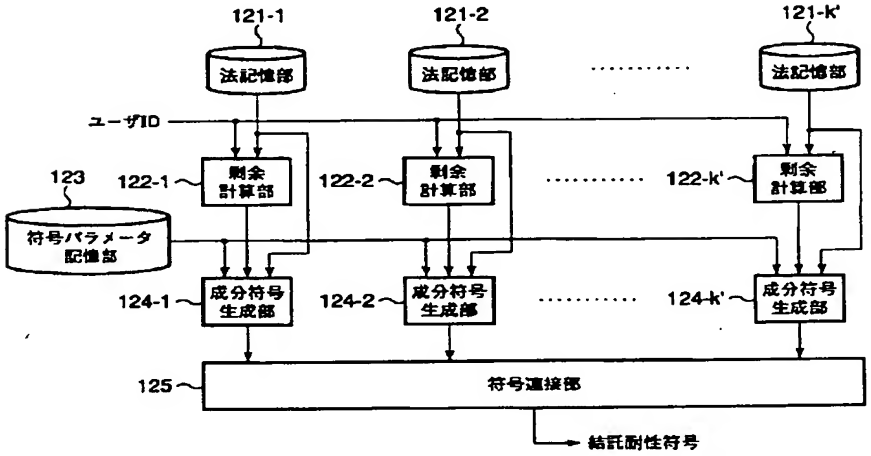
【図５】



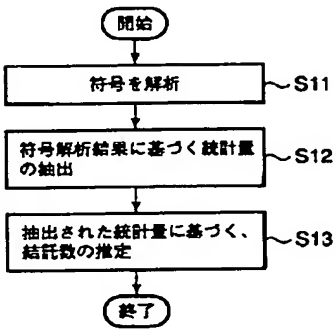
【図６】



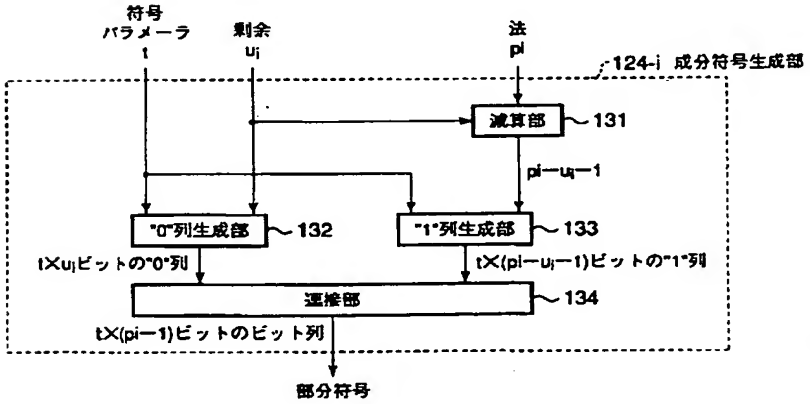
【図７】



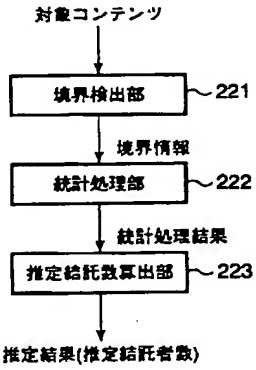
【図１４】



【図８】



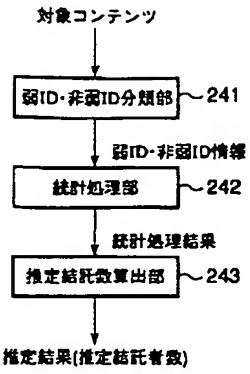
【図１３】



【図９】

ユーザID	B(0)	B(1)	…	B(Smin)	…	B(Smax)	…	B(n-3)	B(n-2)
0	1…1	1…1	1…1	1…1	1…1	1…1	1…1	1…1	1…1
1	0…0	1…1	1…1	1…1	1…1	1…1	1…1	1…1	1…1
…									
Smin	0…0	0…0	0…0	1…1	1…1	1…1	1…1	1…1	1…1
…									
Smax	0…0	0…0	0…0	0…0	0…0	1…1	1…1	1…1	1…1
…									
n-2	0…0	0…0	0…0	0…0	0…0	0…0	0…0	0…0	1…1
n-1	0…0	0…0	0…0	0…0	0…0	0…0	0…0	0…0	0…0

【図１６】



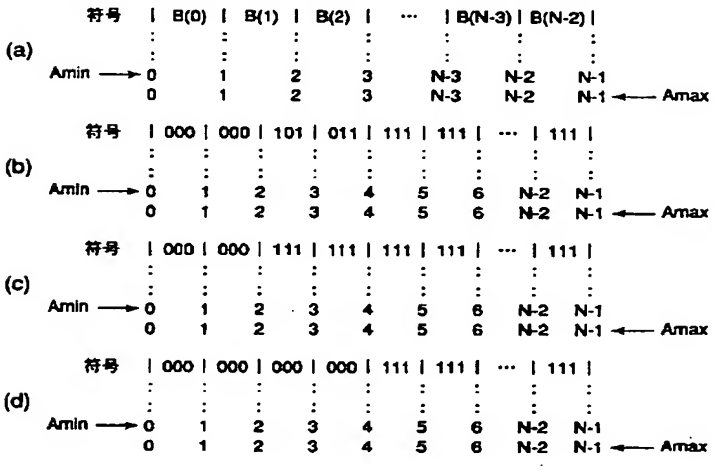
【図１０】

ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
A(1)	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
A(2)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
A(3)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

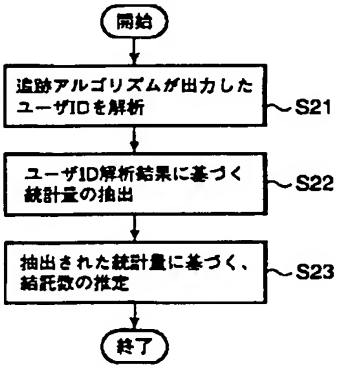
【図１１】

ID	IDに対応する符号(W(1)+W(2)+W(3))		
0	111111	111111111111	1111111111111111
1	000111	000111111111	0001111111111111
2	000000	000000111111	0000001111111111
3	111111	000000000111	0000000001111111
4	000111	000000000000	0000000000001111
5	000000	111111111111	0000000000000111
6	111111	000111111111	0000000000000000
7	000111	000000111111	1111111111111111
8	000000	000000000111	0001111111111111
9	111111	000000000000	0000001111111111
10	000111	111111111111	0000000001111111
11	000000	000111111111	0000000000001111
12	111111	000000111111	0000000000000111
13	000111	000000000111	0000000000000000
14	000000	000000000000	1111111111111111

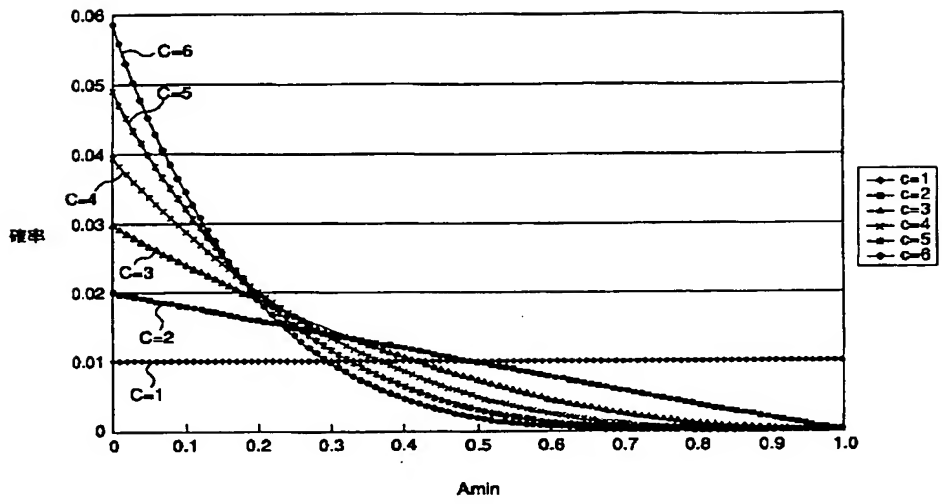
【図１２】



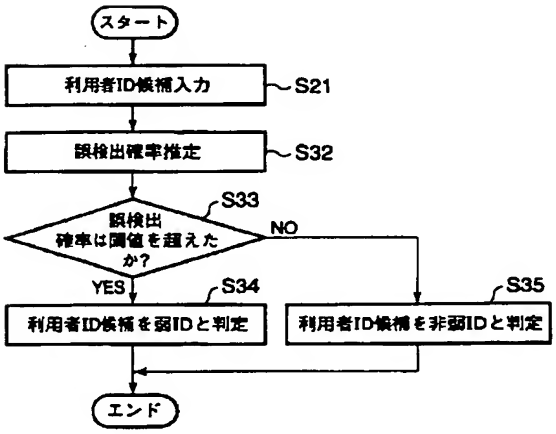
【図１７】



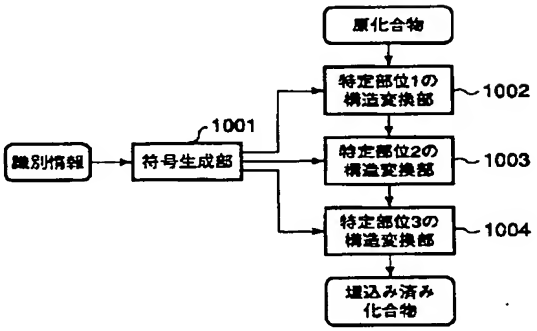
【図１５】



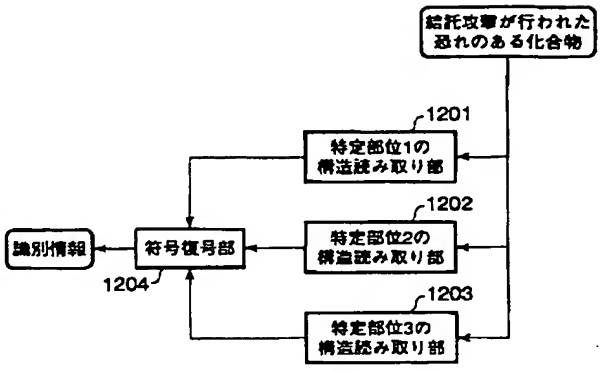
【図１８】



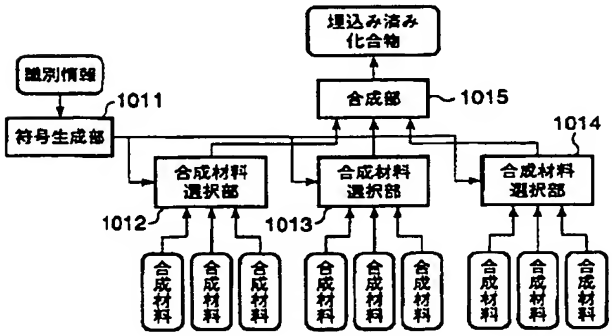
【図１９】



【図２１】



【図２０】



フロントページの続き

(51)Int.Cl.7	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｎ　7/081			